Resource Access Control with Authorization-Certificates[1]

(An Application of Public-key Infrastructure and Digitally Signed Certificates)

William E. Johnston[2], Srilekha Mudumbai, Mary Thompson

Information and Computing Sciences Division

Ernest Orlando Lawrence Berkeley National Laboratory

University of California

[1] This work is supported by the Director, Office of Energy Research, Office of Computation and Technology Research, Mathematical, Information, and Computational Sciences Division, of the U. S. Department of Energy under Contract No. DE-AC03-76SF00098 with the University of California

[2] wejohnston@lbl.gov, 510-486-5014, mudumbai@george.lbl.gov, mrt@george.lbl.gov - http://www-itg.lbl.gov

Security for Widely Distributed Systems - Overall Approach

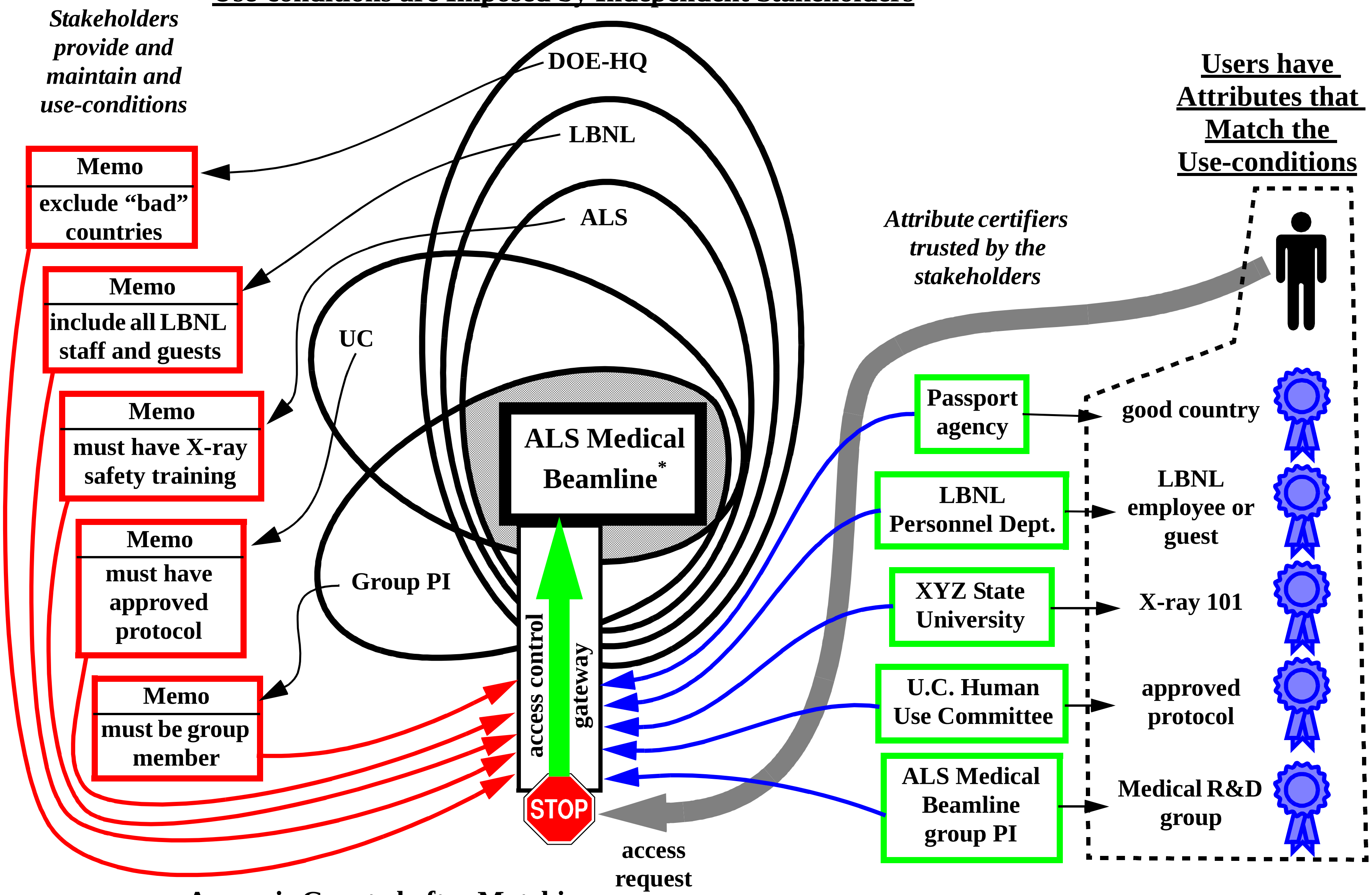
Our scientific environment:

- **multi-user instruments at national facilities**
- **widely distributed supercomputers and large-scale storage systems**
- **data sharing in restricted collaborations**
- **network-based multimedia collaboration channels**

involves facilities, collaboration, and stakeholders that are diffuse: geographically distributed and multi-organizational.

This gives rise to a requirement for distributed management of distributed access control.

Use-conditions are Imposed by Independent Stakeholders



Stakeholders provide and maintain and use-conditions

DOE-HQ

LBNL

ALS

UC

Group PI

Memo
exclude “bad” countries

Memo
include all LBNL staff and guests

Memo
must have X-ray safety training

Memo
must have approved protocol

Memo
must be group member

ALS Medical Beamline[*]

access control gateway

STOP

access request

Users have Attributes that Match the Use-conditions

Attribute certifiers trusted by the stakeholders

Passport agency

LBNL Personnel Dept.

XYZ State University

U.C. Human Use Committee

ALS Medical Beamline group PI

good country

LBNL employee or guest

X-ray 101

approved protocol

Medical R&D group

Access is Granted after Matching Use-conditions and Attributes

[*] hypothetical

Figure 1. Societal Access Control Model

Goals

Capabilities and tools in our computing and communications environment that reflect the societal model:

- **stakeholders independently make assertions**
- **dynamic and easily used mechanisms**
- **strong assurances**

The General Security Model for Access Control

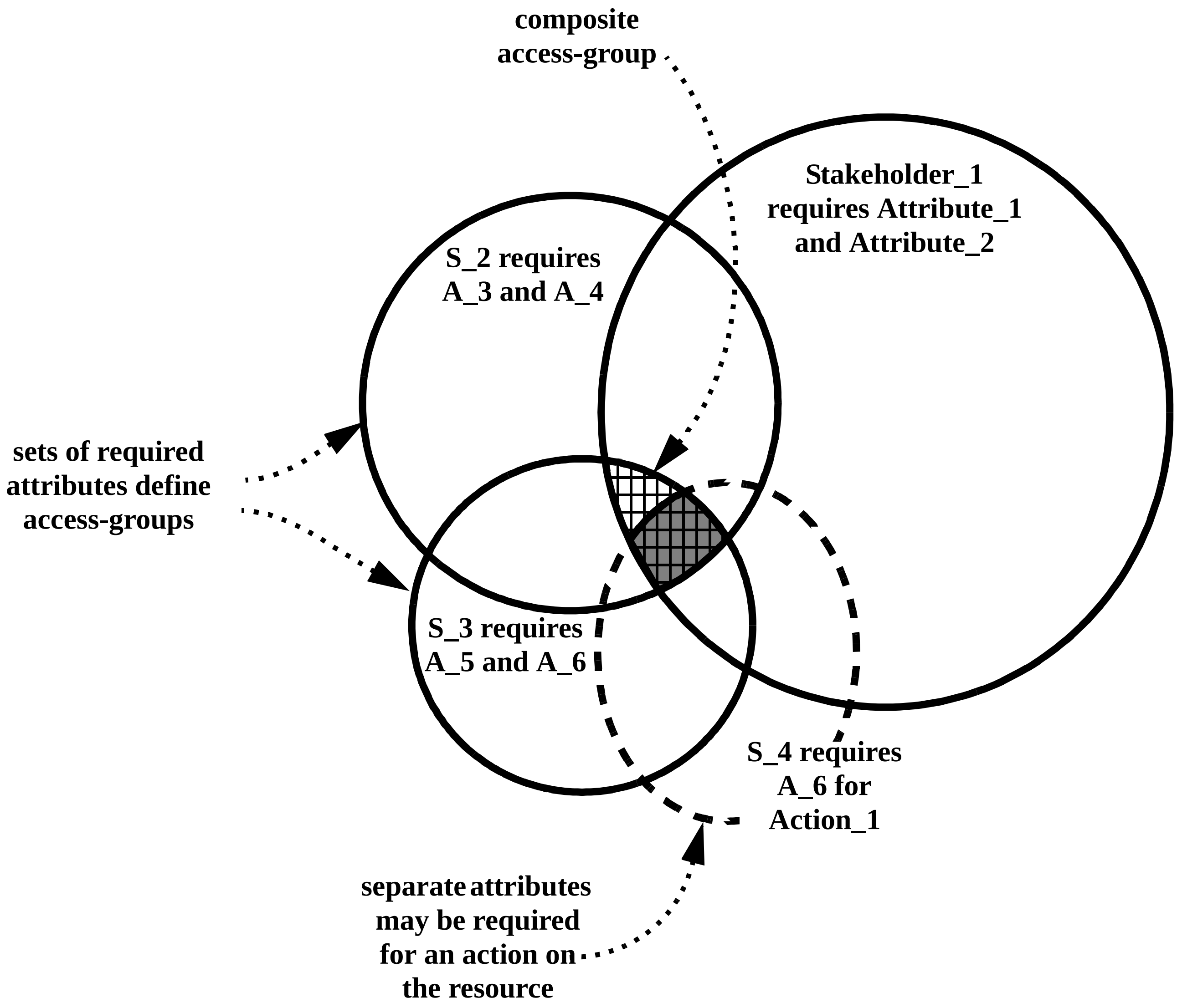
The goal of the security model is to be able to support a variety of policy models, including flat and hierarchical authority, and decentralized and centralized management of access rights.

The security model provides for controlling access to resources via restrictions imposed by several types of use-conditions that are defined independently by multiple stakeholders:

- access groups are defined implicitly by requiring a set of attributes
- actions on resources may be further restricted by requiring additional attributes (evaluated independently of access)
- operational requirements (e.g. time-of-day) are defined and satisfied by “data fields” in attribute certificates

These use-conditions are satisfied by (certified) attributes of those entities trying to gain access to resources.

Security Model



composite
access-group

Stakeholder_1
requires Attribute_1
and Attribute_2

S_2 requires
A_3 and A_4

sets of required
attributes define
access-groups

S_3 requires
A_5 and A_6

S_4 requires
A_6 for
Action_1

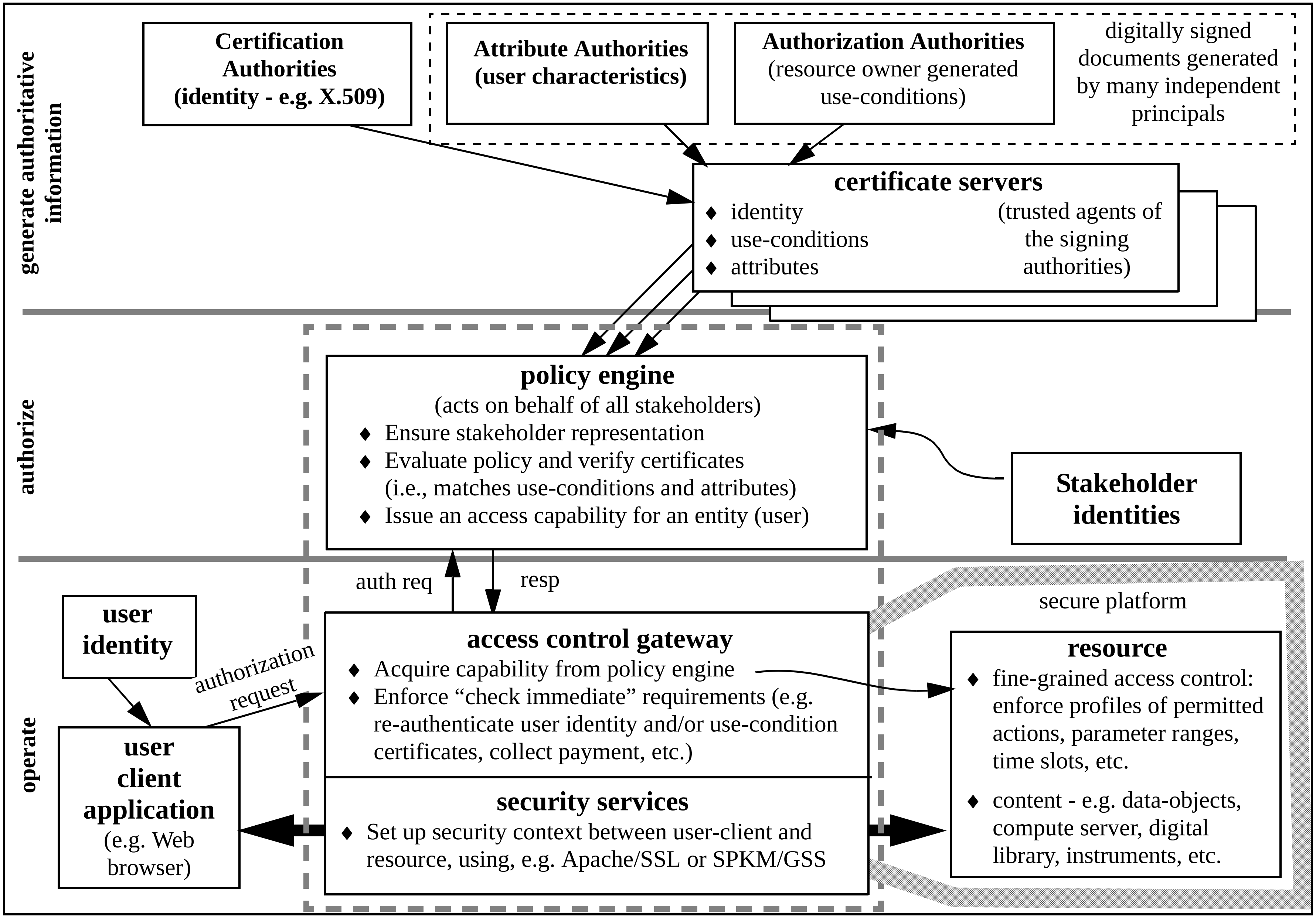
separate attributes
may be required
for an action on
the resource

Access Groups are Defined by Several Required Attributes

Approach

- ♦ **Architecture:**
  - **data driven certificate analysis (no semantic analysis of the use-conditions)**
  - **user capability (verified, required attributes) are provided to the protected resource to enable fine-grained control**
  - **existing services provide end-to-end security**
- ♦ **Certificate management**

Approach



generate authoritative information

Certification Authorities (identity - e.g. X.509)

Attribute Authorities (user characteristics)

Authorization Authorities (resource owner generated use-conditions)

digitally signed documents generated by many independent principals

certificate servers

- ♦ identity
- ♦ use-conditions
- ♦ attributes

(trusted agents of the signing authorities)

authorize

policy engine

(acts on behalf of all stakeholders)

- ♦ Ensure stakeholder representation
- ♦ Evaluate policy and verify certificates (i.e., matches use-conditions and attributes)
- ♦ Issue an access capability for an entity (user)

Stakeholder identities

operate

auth req

resp

user identity

authorization request

user client application (e.g. Web browser)

access control gateway

- ♦ Acquire capability from policy engine
- ♦ Enforce “check immediate” requirements (e.g. re-authenticate user identity and/or use-condition certificates, collect payment, etc.)

security services

- ♦ Set up security context between user-client and resource, using, e.g. Apache/SSL or SPKM/GSS

secure platform

resource

- ♦ fine-grained access control: enforce profiles of permitted actions, parameter ranges, time slots, etc.
- ♦ content - e.g. data-objects, compute server, digital library, instruments, etc.

Figure 2. The Overall Architecture of the Authorization Certificate Approach

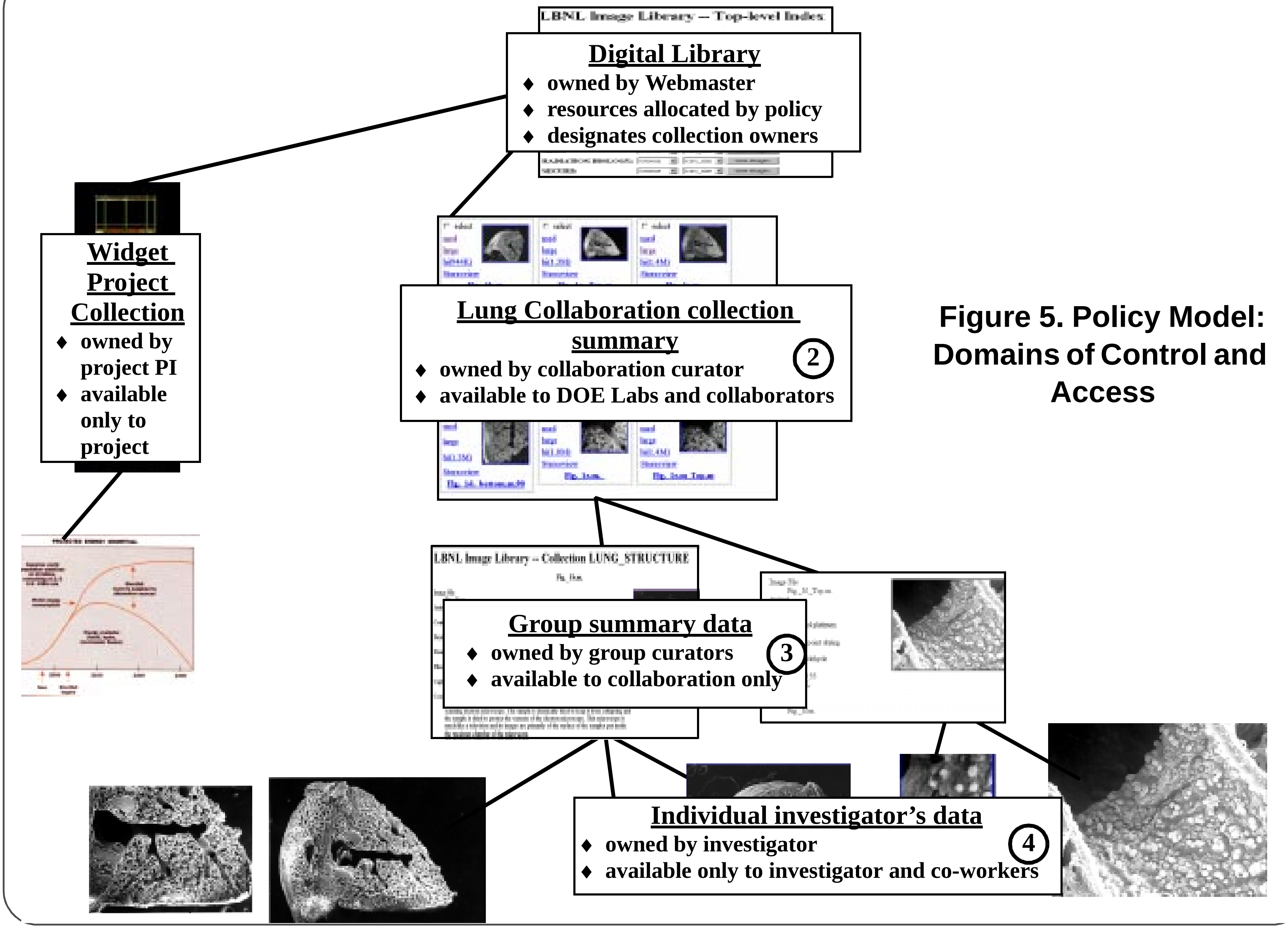
Policy Model

Policy Model

A *policy model* is built on a general security model in a way that will support the access policies needed in a particular resource domain.

The characteristics of a particular policy model - e.g. hierarchical authority with delegation - is a function of the resource / application domain.

Policy Model



LBNL Image Library -- Top-level Index

Digital Library

- owned by Webmaster
- resources allocated by policy
- designates collection owners

Widget Project Collection

- owned by project PI
- available only to project

Lung Collaboration collection summary 2

- owned by collaboration curator
- available to DOE Labs and collaborators

LBNL Image Library -- Collection LUNG_STRUCTURE

Group summary data 3

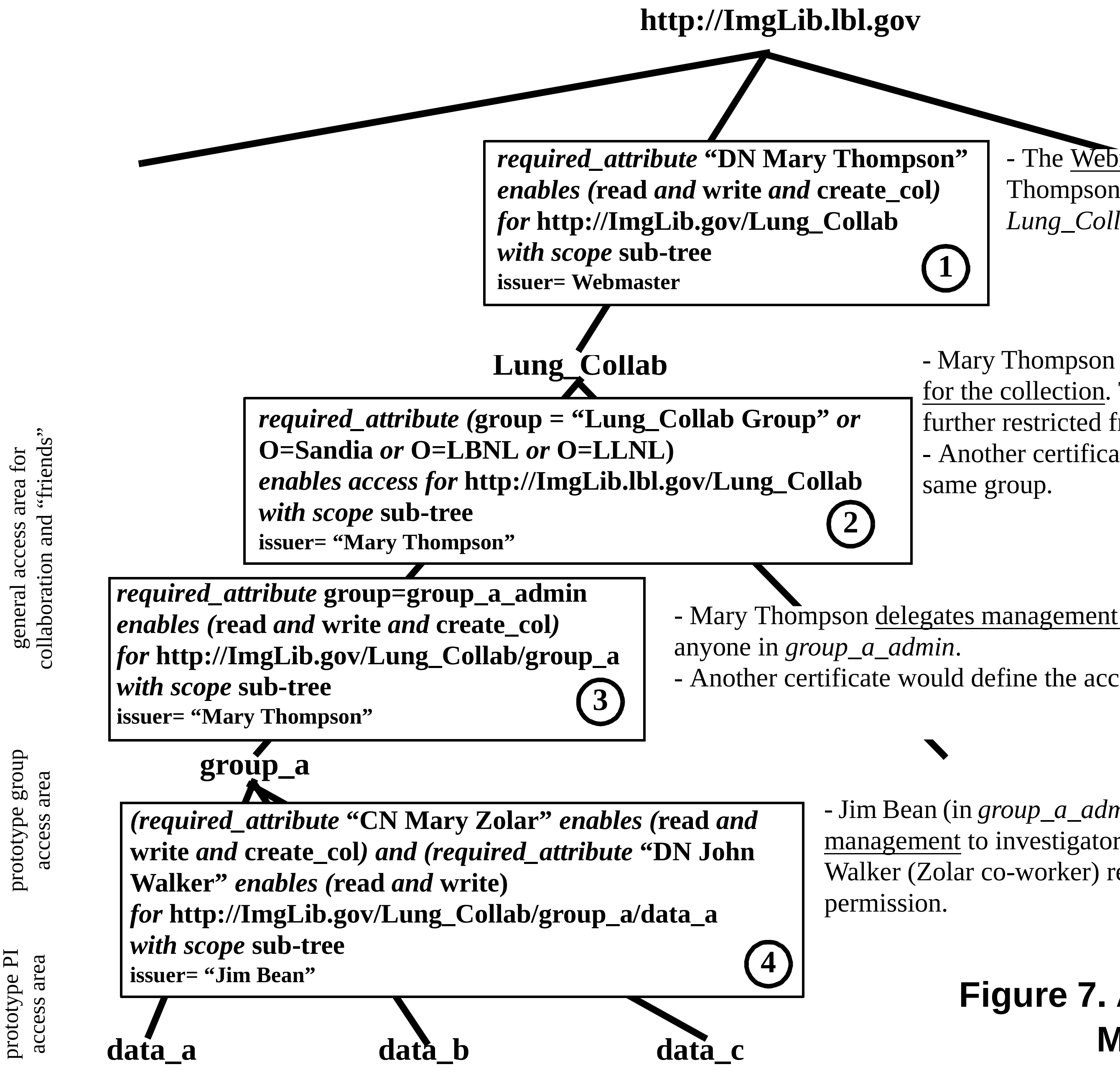
- owned by group curators
- available to collaboration only

Individual investigator's data 4

- owned by investigator
- available only to investigator and co-workers

Figure 5. Policy Model: Domains of Control and Access

Policy Model



http://ImgLib.lbl.gov

***required_attribute* “DN Mary Thompson”**
enables (*read *and* write *and* create_col*)
***for* http://ImgLib.gov/Lung_Collab**
***with scope* sub-tree**
issuer= Webmaster
1

- The Webmaster delegates to Mary Thompson the authority to manage the *Lung_Collab* collection.

Lung_Collab

***required_attribute* (group = “Lung_Collab Group” *or* O=Sandia *or* O=LBNL *or* O=LLNL)**
***enables access for* http://ImgLib.lbl.gov/Lung_Collab**
***with scope* sub-tree**
issuer= “Mary Thompson”
2

- Mary Thompson establishes the general access group for the collection. This access group may only be further restricted from this point down.
- Another certificate at this level grants *read* to this same group.

general access area for collaboration and “friends”

***required_attribute* group=group_a_admin**
enables (*read *and* write *and* create_col*)
***for* http://ImgLib.gov/Lung_Collab/group_a**
***with scope* sub-tree**
issuer= “Mary Thompson”
3

- Mary Thompson delegates management of the *group_a* collection to anyone in *group_a_admin*.
- Another certificate would define the access group as *Lung_Collab* only.

group_a

prototype group access area

***(required_attribute* “CN Mary Zolar” *enables (*read *and* write *and* create_col*) and (required_attribute* “DN John Walker” *enables (*read *and* write)**
***for* http://ImgLib.gov/Lung_Collab/group_a/data_a**
***with scope* sub-tree**
issuer= “Jim Bean”
4

- Jim Bean (in *group_a_admin*) delegates *data_a* collection management to investigator Mary Zolar and grants John Walker (Zolar co-worker) read and write (object create) permission.

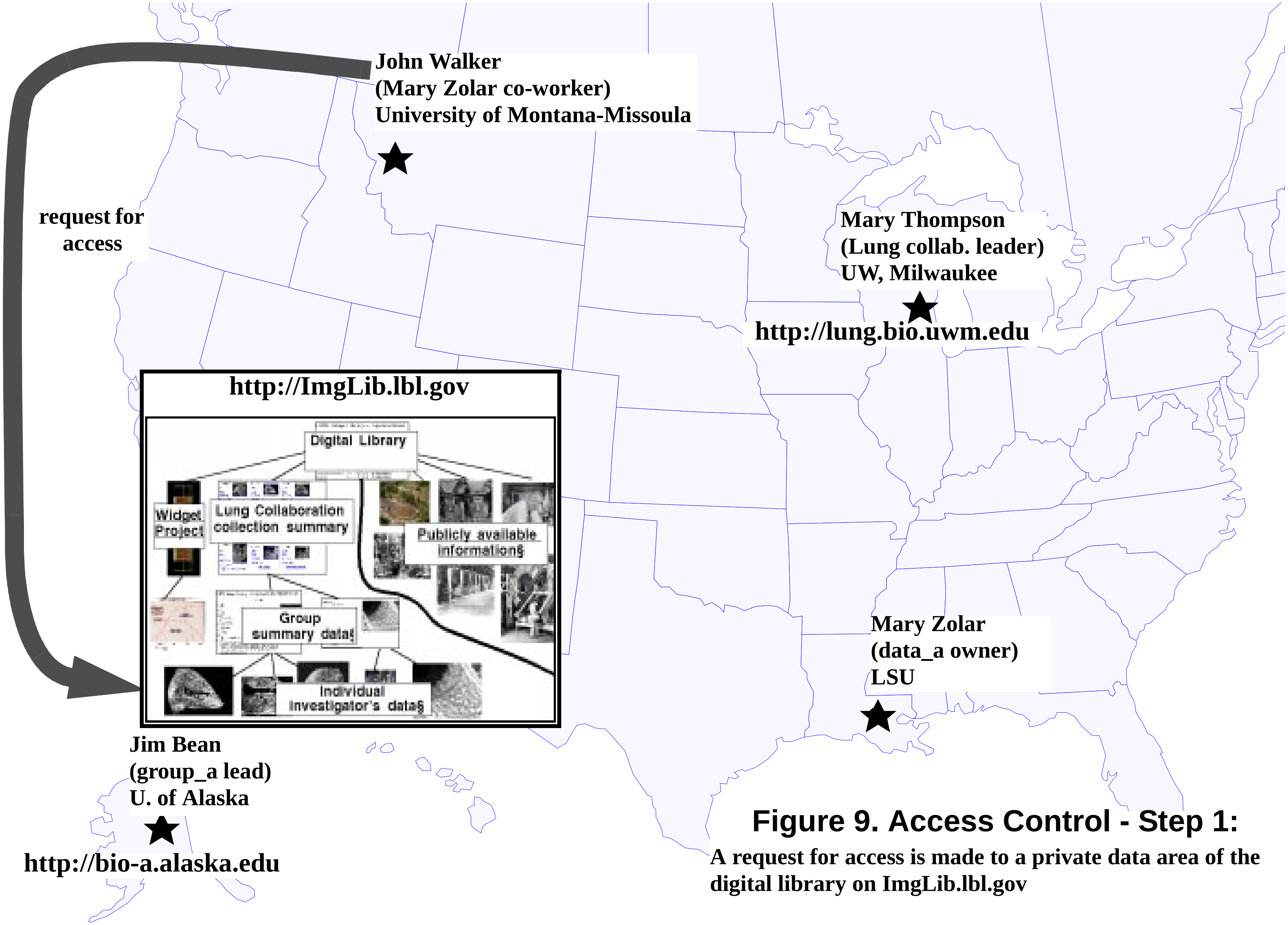
prototype PI access area

data_a **data_b** **data_c**

Figure 7. Access Control Policy Model Example

Example

The following figures illustrate the flow of control and information in the Akenti access control system.



John Walker
(Mary Zolar co-worker)
University of Montana-Missoula

request for
access

Mary Thompson
(Lung collab. leader)
UW, Milwaukee

http://lung.bio.uwm.edu

http://ImgLib.lbl.gov

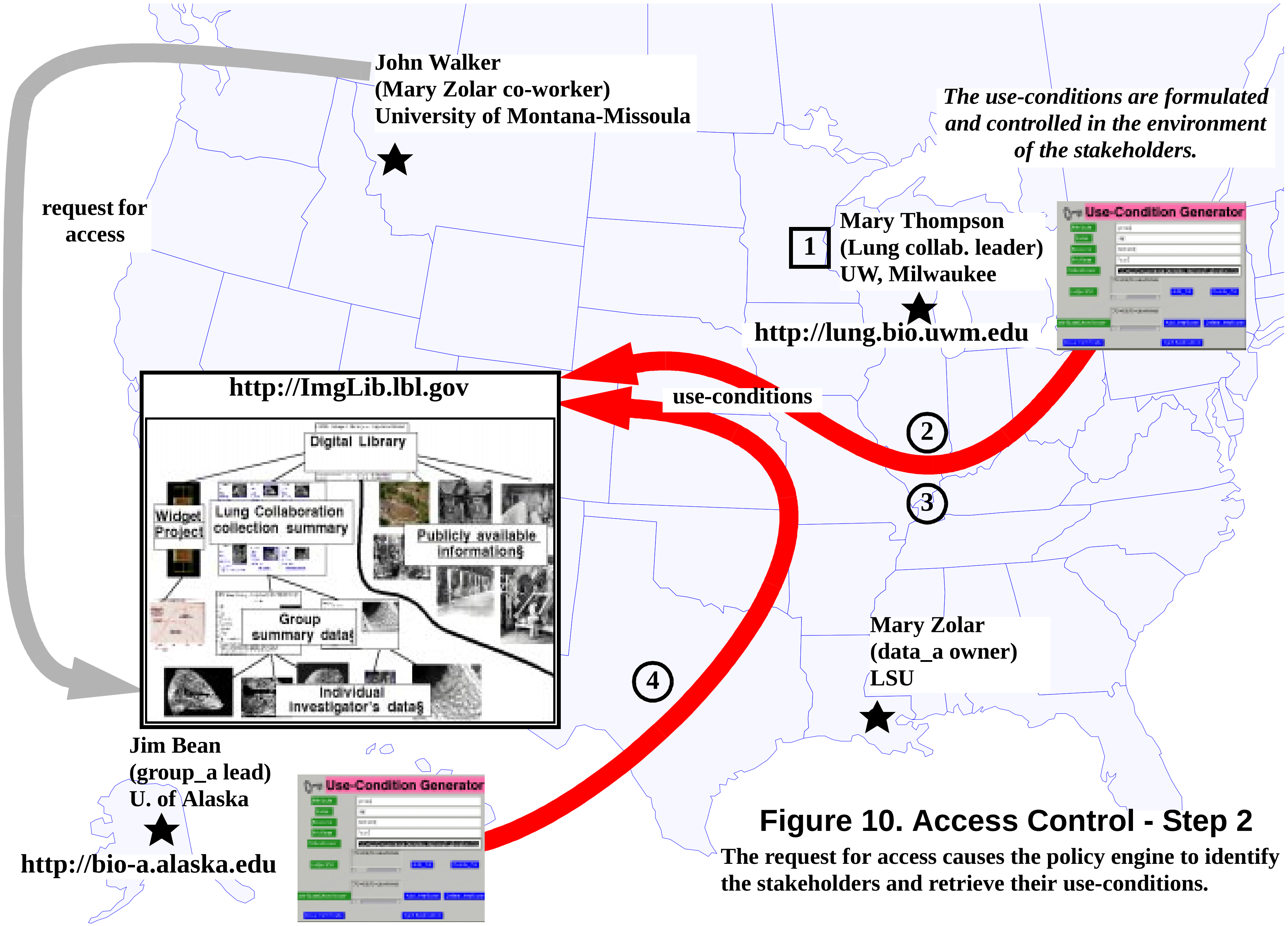
Digital Library
Widget Project
Lung Collaboration collection summary
Publicly available information§
Group summary data§
Individual investigator's data§

Mary Zolar
(data_a owner)
LSU

Jim Bean
(group_a lead)
U. of Alaska

http://bio-a.alaska.edu

Figure 9. Access Control - Step 1:
A request for access is made to a private data area of the digital library on ImgLib.lbl.gov



John Walker
(Mary Zolar co-worker)
University of Montana-Missoula

The use-conditions are formulated and controlled in the environment of the stakeholders.

request for access

Mary Thompson
(Lung collab. leader)
UW, Milwaukee

http://lung.bio.uwm.edu

http://ImgLib.lbl.gov

use-conditions

Mary Zolar
(data_a owner)
LSU

Jim Bean
(group_a lead)
U. of Alaska

http://bio-a.alaska.edu

1
2
3
4
Use-Condition Generator
Digital Library
Widget Project
Lung Collaboration collection summary
Publicly available information
Group summary data
Individual investigator's data
Use-Condition Generator

Figure 10. Access Control - Step 2

The request for access causes the policy engine to identify the stakeholders and retrieve their use-conditions.

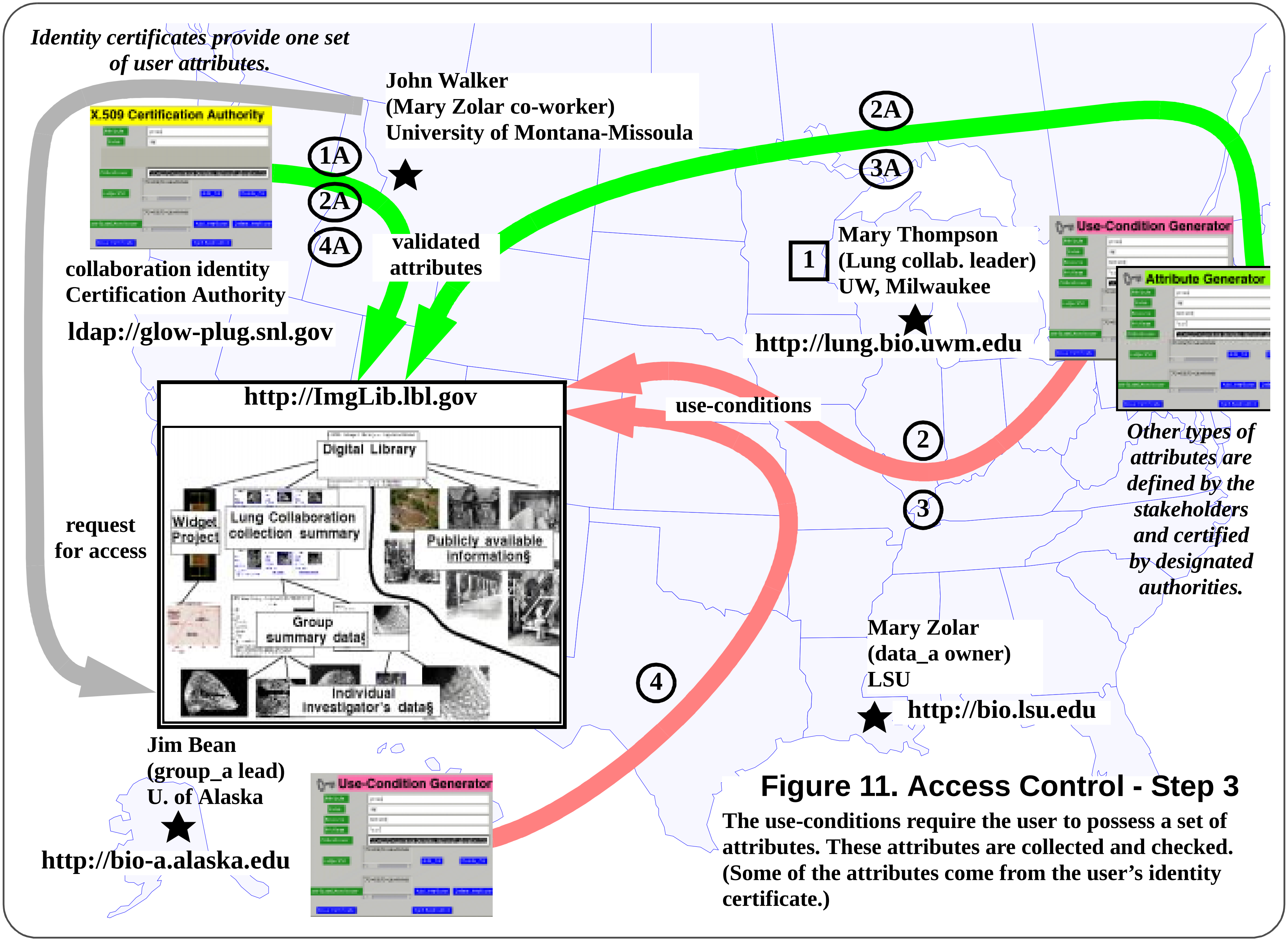


Figure 11. Access Control - Step 3

The use-conditions require the user to possess a set of attributes. These attributes are collected and checked. (Some of the attributes come from the user's identity certificate.)

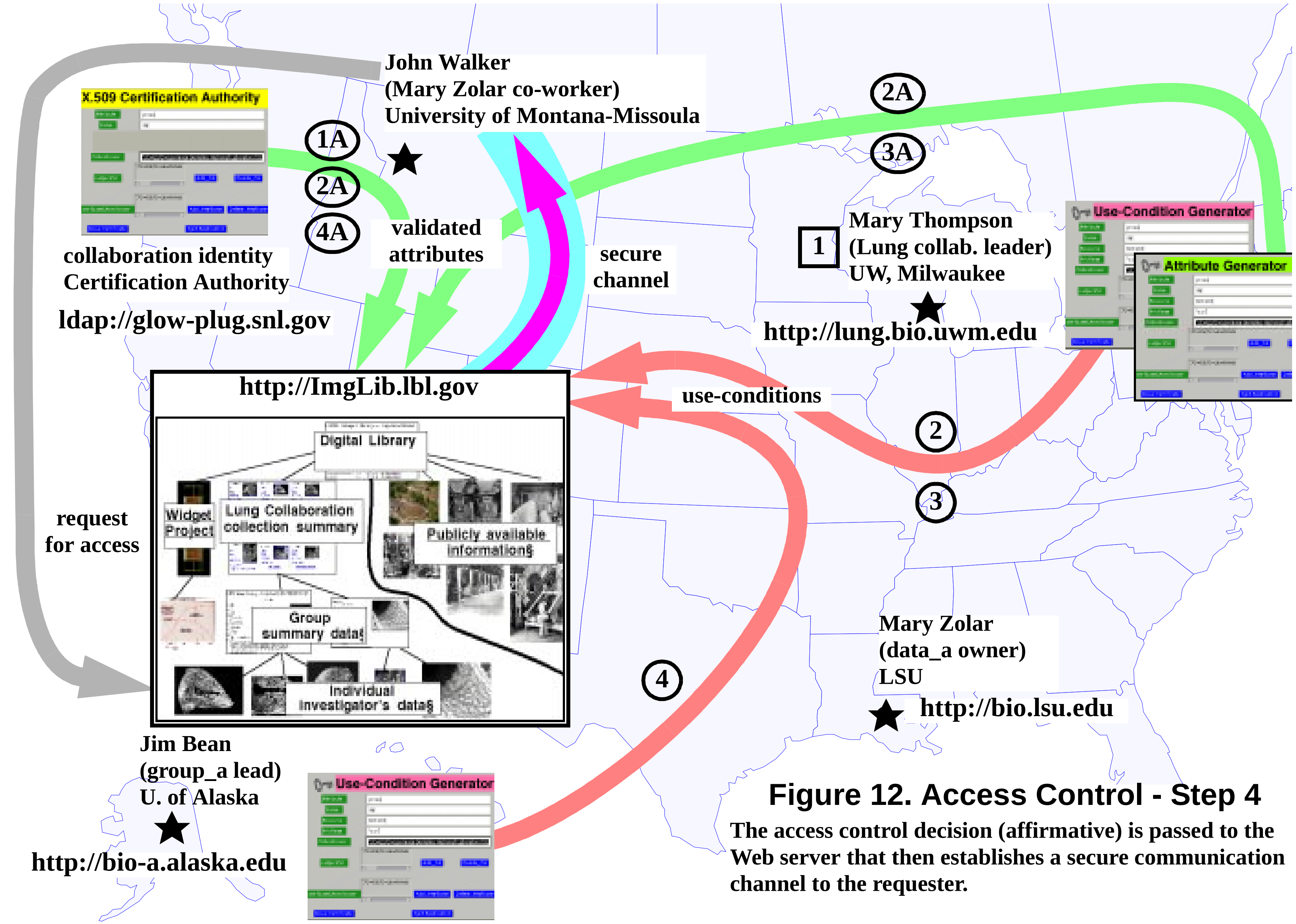


Figure 12. Access Control - Step 4

The access control decision (affirmative) is passed to the Web server that then establishes a secure communication channel to the requester.

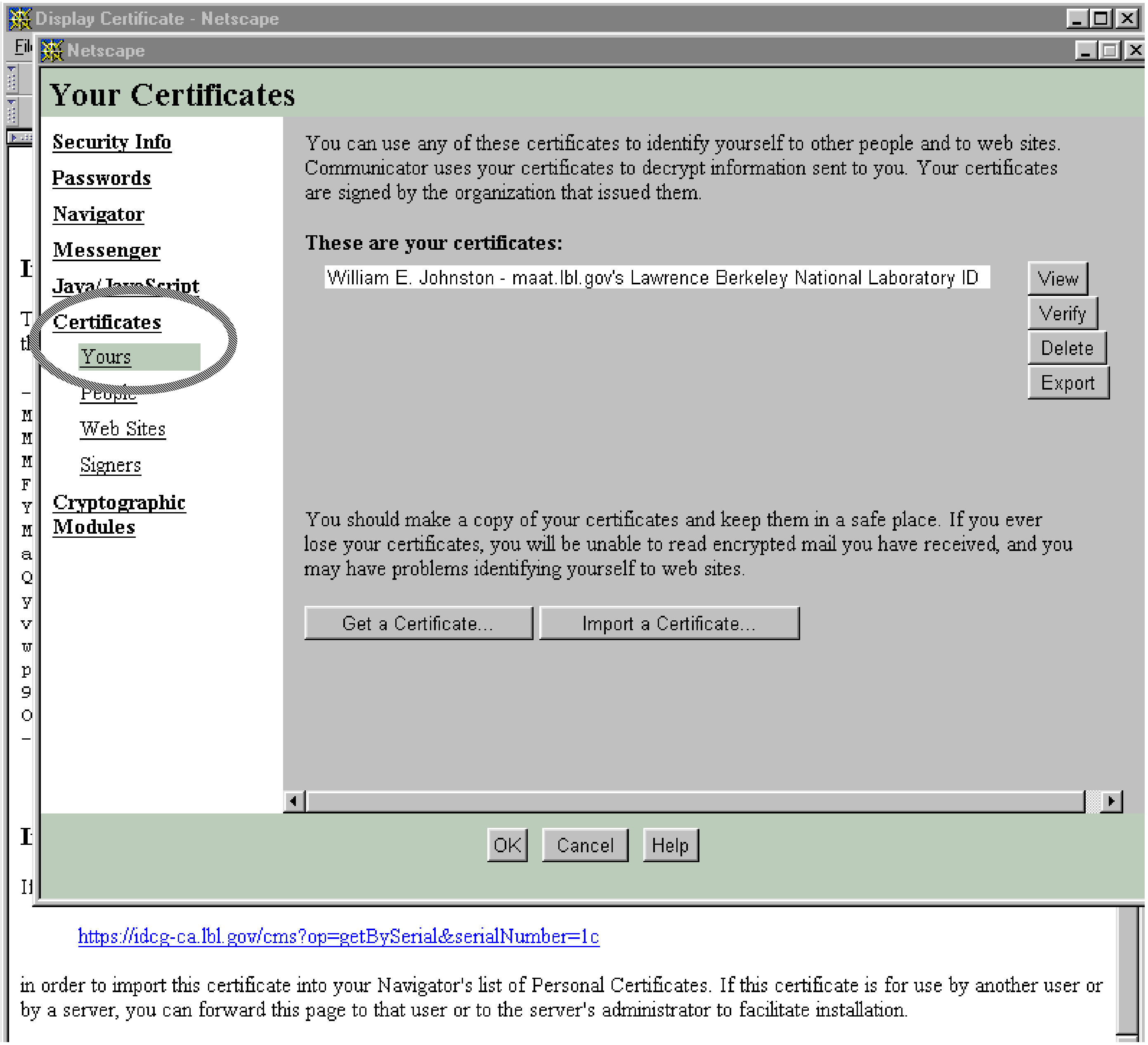
Certificate Infrastructure

How are certificates generated and managed is a key factor for the usability of the access control system.

- Must be very simple for the user
- Must be relatively simple for stakeholders
- Must not be an administrative burden

Netscape has built a nice collection of certificate management tools and user interfaces, and our implementation uses these facilities.

Certificate Infrastructure



Your Certificates

You can use any of these certificates to identify yourself to other people and to web sites. Communicator uses your certificates to decrypt information sent to you. Your certificates are signed by the organization that issued them.

These are your certificates:

William E. Johnston - maat.lbl.gov's Lawrence Berkeley National Laboratory ID

You should make a copy of your certificates and keep them in a safe place. If you ever lose your certificates, you will be unable to read encrypted mail you have received, and you may have problems identifying yourself to web sites.

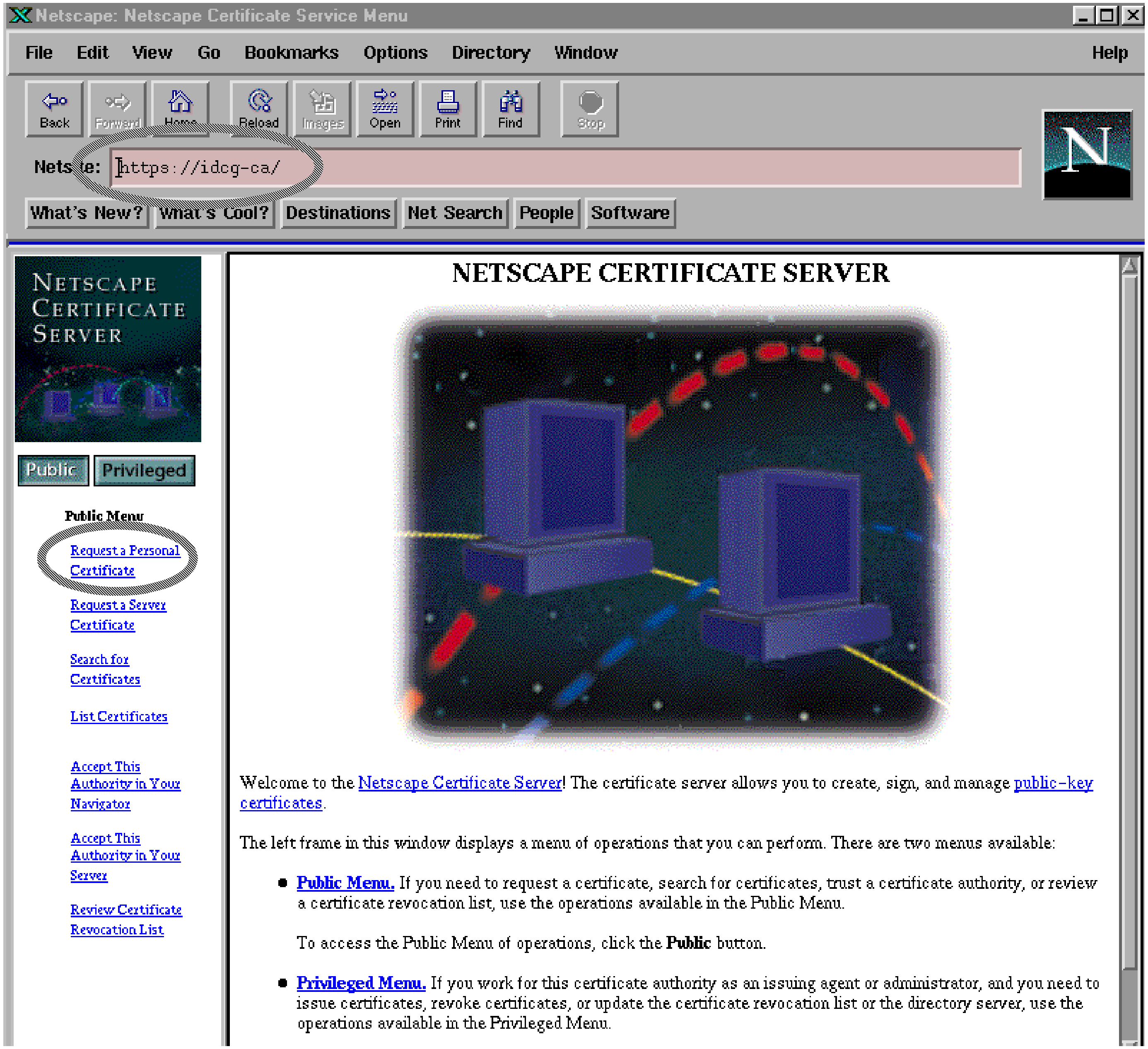
https://idcg-ca.lbl.gov/cms?op=getBySerial&serialNumber=1c

in order to import this certificate into your Navigator's list of Personal Certificates. If this certificate is for use by another user or by a server, you can forward this page to that user or to the server's administrator to facilitate installation.

The Netscape 4 / Communicator security interface - after an identity certificate has been installed.

In general, users will probably have several identities.

Certificate Infrastructure


Netscape: Netscape Certificate Service Menu
File
Edit
View
Go
Bookmarks
Options
Directory
Window
Help
Back
Forward
Home
Reload
Images
Open
Print
Find
Stop
Netsite:
What's New?
What's Cool?
Destinations
Net Search
People
Software
NETSCAPE CERTIFICATE SERVER
Public
Privileged
Public Menu
Request a Personal Certificate
Request a Server Certificate
Search for Certificates
List Certificates
Accept This Authority in Your Navigator
Accept This Authority in Your Server
Review Certificate Revocation List

https://idcg-ca/

NETSCAPE CERTIFICATE SERVER

Welcome to the Netscape Certificate Server! The certificate server allows you to create, sign, and manage public-key certificates.

The left frame in this window displays a menu of operations that you can perform. There are two menus available:

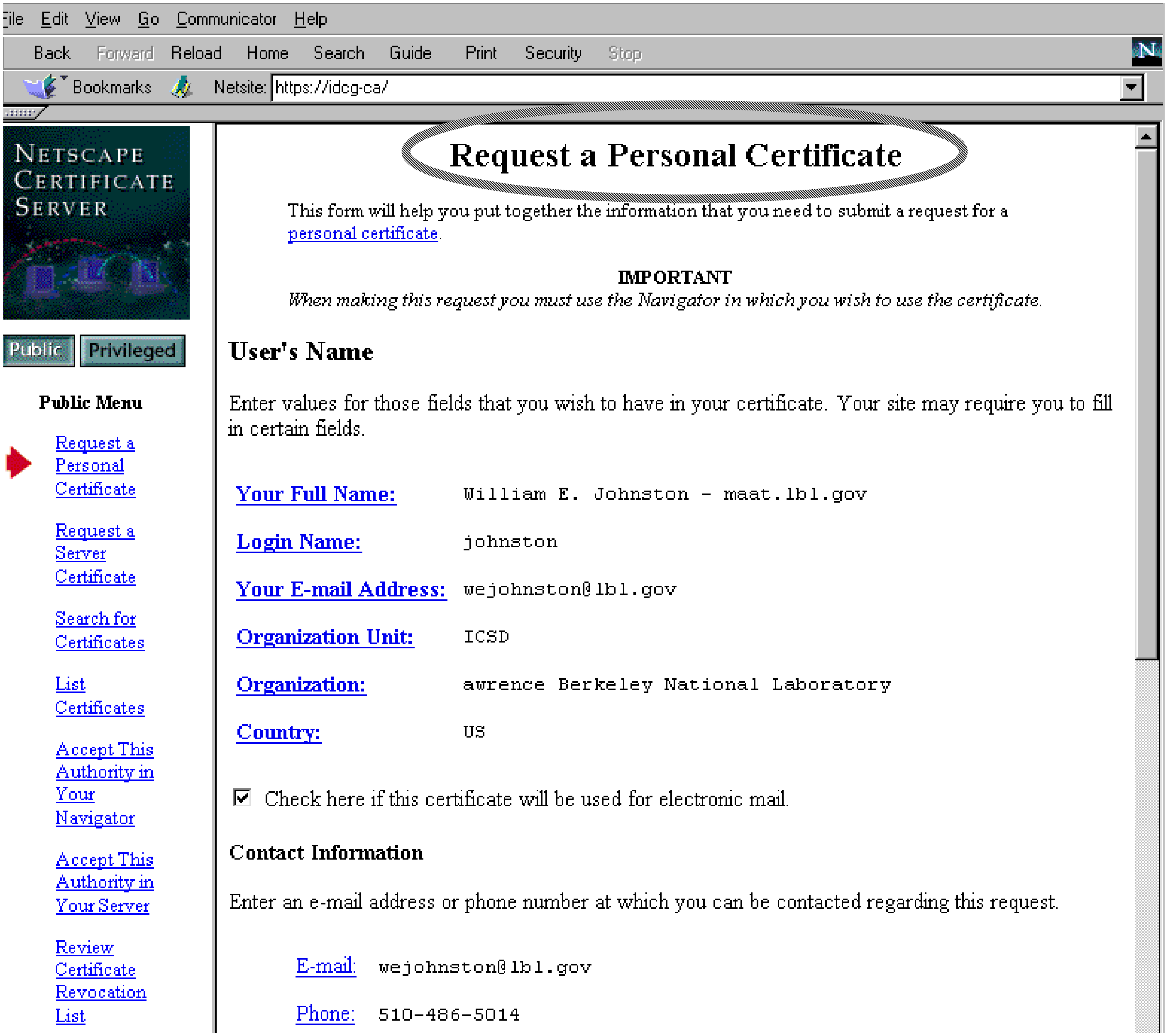
- **Public Menu.** If you need to request a certificate, search for certificates, trust a certificate authority, or review a certificate revocation list, use the operations available in the Public Menu.

  To access the Public Menu of operations, click the **Public** button.

- **Privileged Menu.** If you work for this certificate authority as an issuing agent or administrator, and you need to issue certificates, revoke certificates, or update the certificate revocation list or the directory server, use the operations available in the Privileged Menu.

Establish user identity: the request to the certification authority.

Certificate Infrastructure



File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Netsite: https://idcg-ca/
NETSCAPE CERTIFICATE SERVER
Public Privileged
Public Menu
Request a Personal Certificate
Request a Server Certificate
Search for Certificates
List Certificates
Accept This Authority in Your Navigator
Accept This Authority in Your Server
Review Certificate Revocation List

Request a Personal Certificate

This form will help you put together the information that you need to submit a request for a personal certificate.

IMPORTANT

When making this request you must use the Navigator in which you wish to use the certificate.

User's Name

Enter values for those fields that you wish to have in your certificate. Your site may require you to fill in certain fields.

Your Full Name:	William E. Johnston - maat.lbl.gov
Login Name:	johnston
Your E-mail Address:	wejohnston@lbl.gov
Organization Unit:	ICSD
Organization:	awrence Berkeley National Laboratory
Country:	US

☑ Check here if this certificate will be used for electronic mail.

Contact Information

Enter an e-mail address or phone number at which you can be contacted regarding this request.

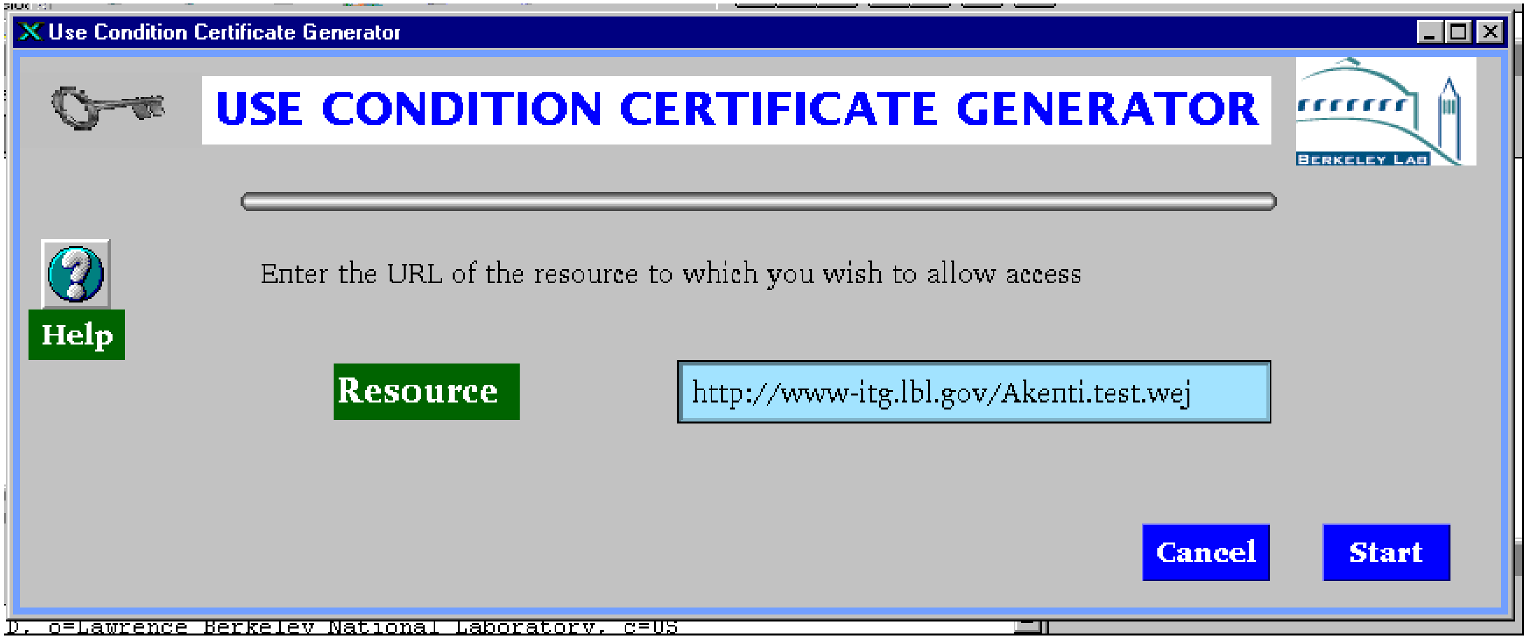
E-mail:	wejohnston@lbl.gov
Phone:	510-486-5014

Certificate Infrastructure

- ♦ **Stakeholder interaction**

Use-condition certificates specify a set of attributes that must be presented in order to allow access to, and actions on a resource.

Certificate Infrastructure



Use Condition Certificate Generator

USE CONDITION CERTIFICATE GENERATOR

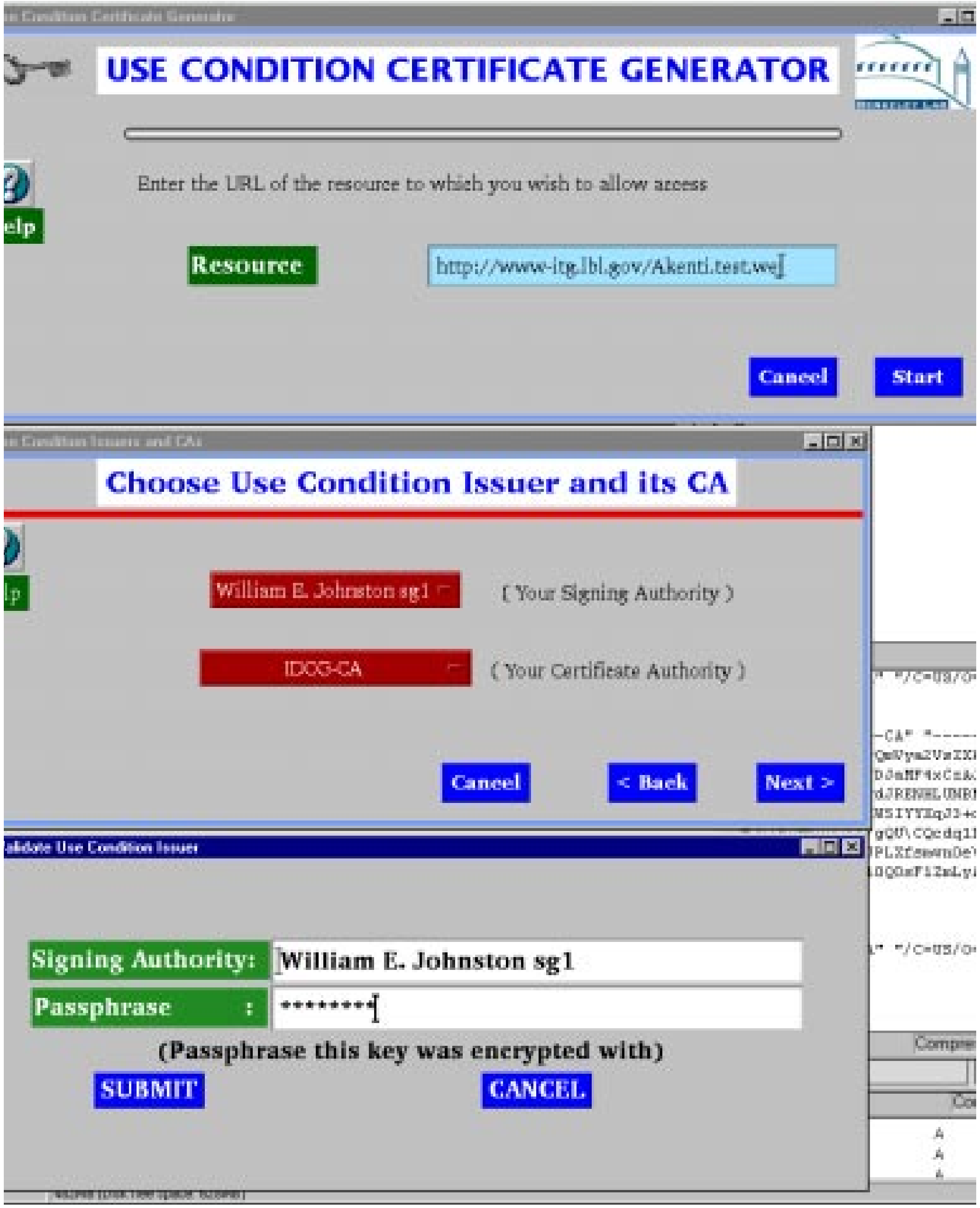
Enter the URL of the resource to which you wish to allow access

Resource: http://www-itg.lbl.gov/Akenti.test.wej

D, o=Lawrence Berkeley National Laboratory, c=US

- **By naming the resource, the use-condition issuers (stakeholders) are identified (the .*htauthority* file for the resource is retrieved)**
- **Authority scoping is dependent on the nature of the resource policy model. For Web servers scoping is established by the location of the stakeholder in the directory hierarchy.**

Certificate Infrastructure



USE CONDITION CERTIFICATE GENERATOR

Enter the URL of the resource to which you wish to allow access

Resource: http://www-itg.lbl.gov/Akenti.test.we

Choose Use Condition Issuer and its CA

William E. Johnston sg1 (Your Signing Authority)

IDCG-CA (Your Certificate Authority)

alidate Use Condition Issuer

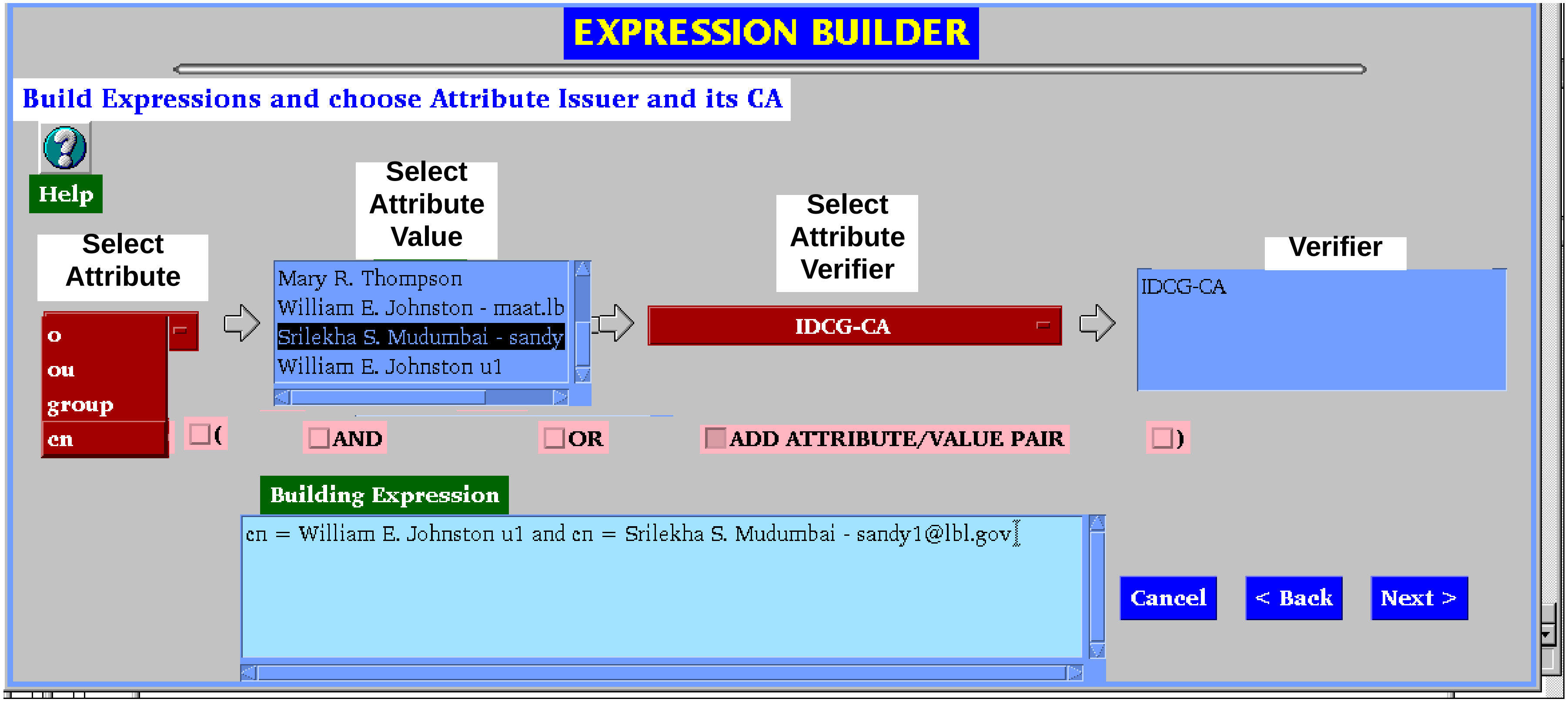
Signing Authority: William E. Johnston sg1

Passphrase : ********

(Passphrase this key was encrypted with)

- Pick the stakeholder persona that will issue this use condition and unlock the signing key

Certificate Infrastructure



EXPRESSION BUILDER

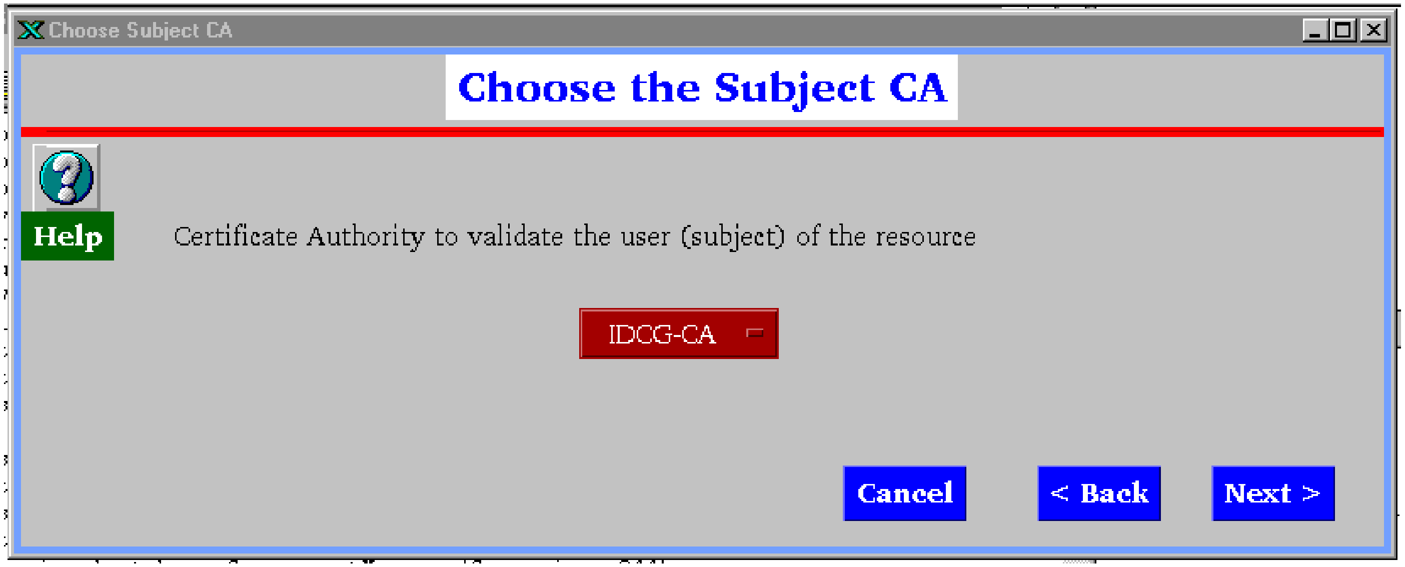
Build Expressions and choose Attribute Issuer and its CA

Building Expression: cn = William E. Johnston u1 and cn = Srilekha S. Mudumbai - sandy1@lbl.gov

- ♦ The use-condition certificate specifies required attributes and values, together with who is trusted to attest to those attributes.

- ♦ Attributes may be arbitrary name-value pairs, or a component of an X.509 distinguished name.

Certificate Infrastructure



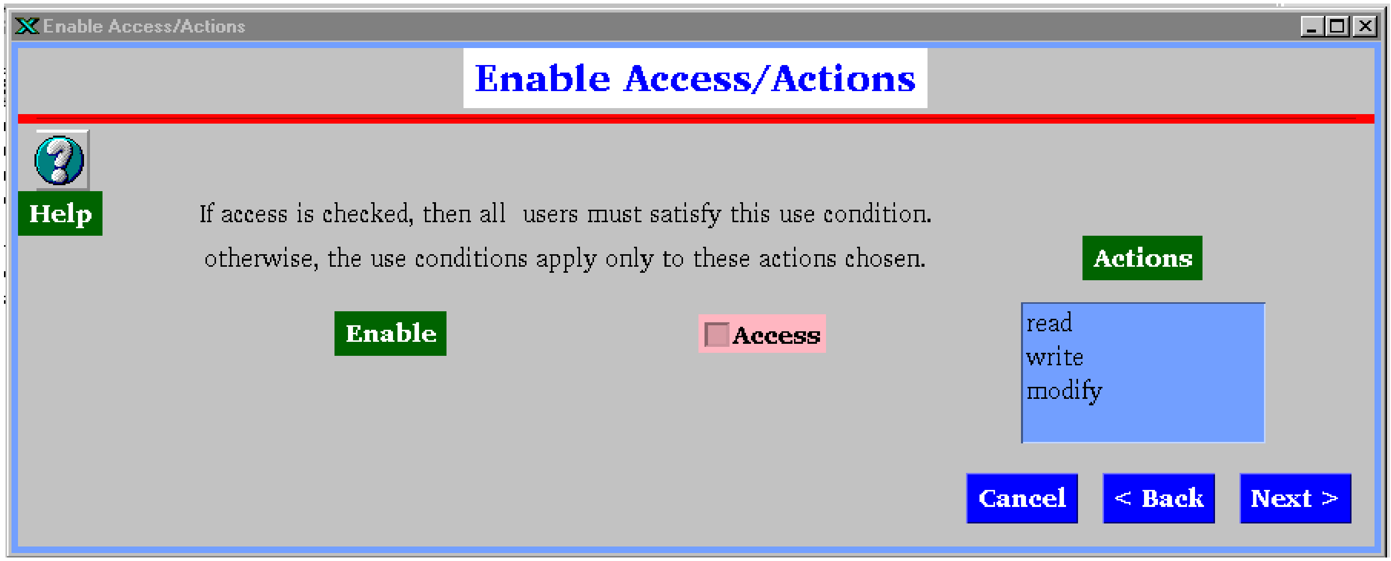
Choose the Subject CA

Certificate Authority to validate the user (subject) of the resource

IDCG-CA

- ♦ **If the required attribute is from an X.509 certificate, then the CA of the user is that which issued the identity certificate**
- ♦ **If the required attribute is defined by the stakeholder, then the identity verifier of the user must be separately specified.**

Certificate Infrastructure

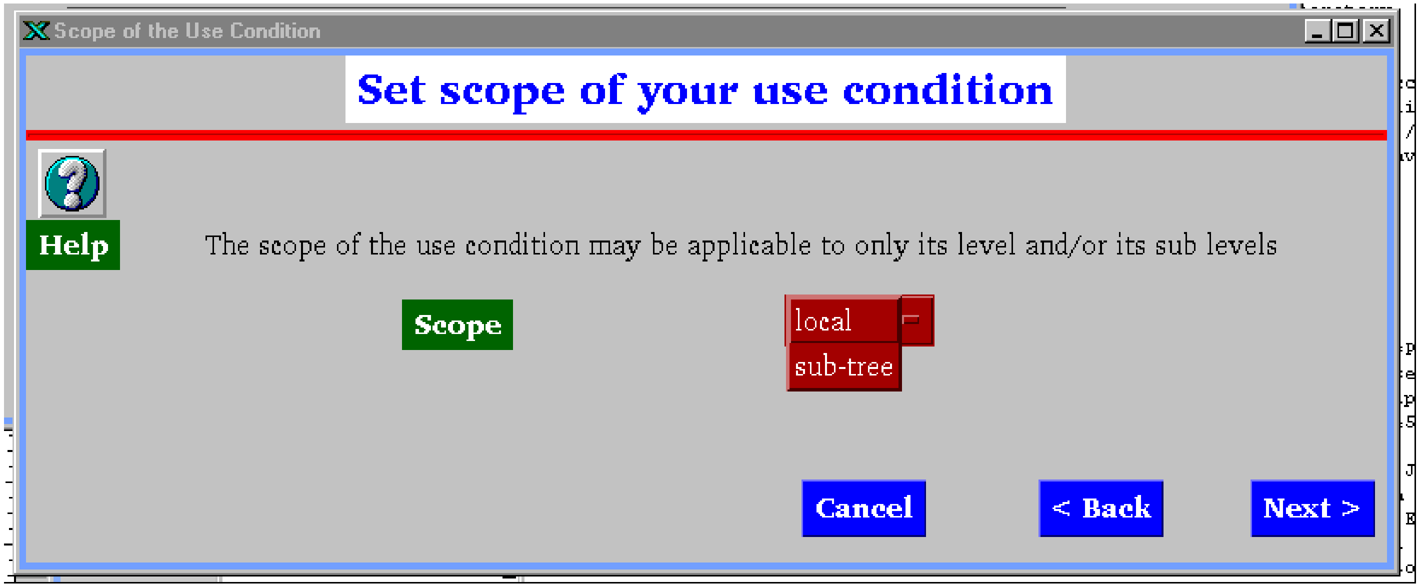


If access is checked, then all users must satisfy this use condition.

otherwise, the use conditions apply only to these actions chosen.

- In addition to undifferentiated access rights, the use-condition certificate can encode qualifications on actions. The policy engine extracts the permitted “actions” as uninterpreted keywords and passes them to the resource server where the action keywords are associated with methods that act on the resource.

Certificate Infrastructure



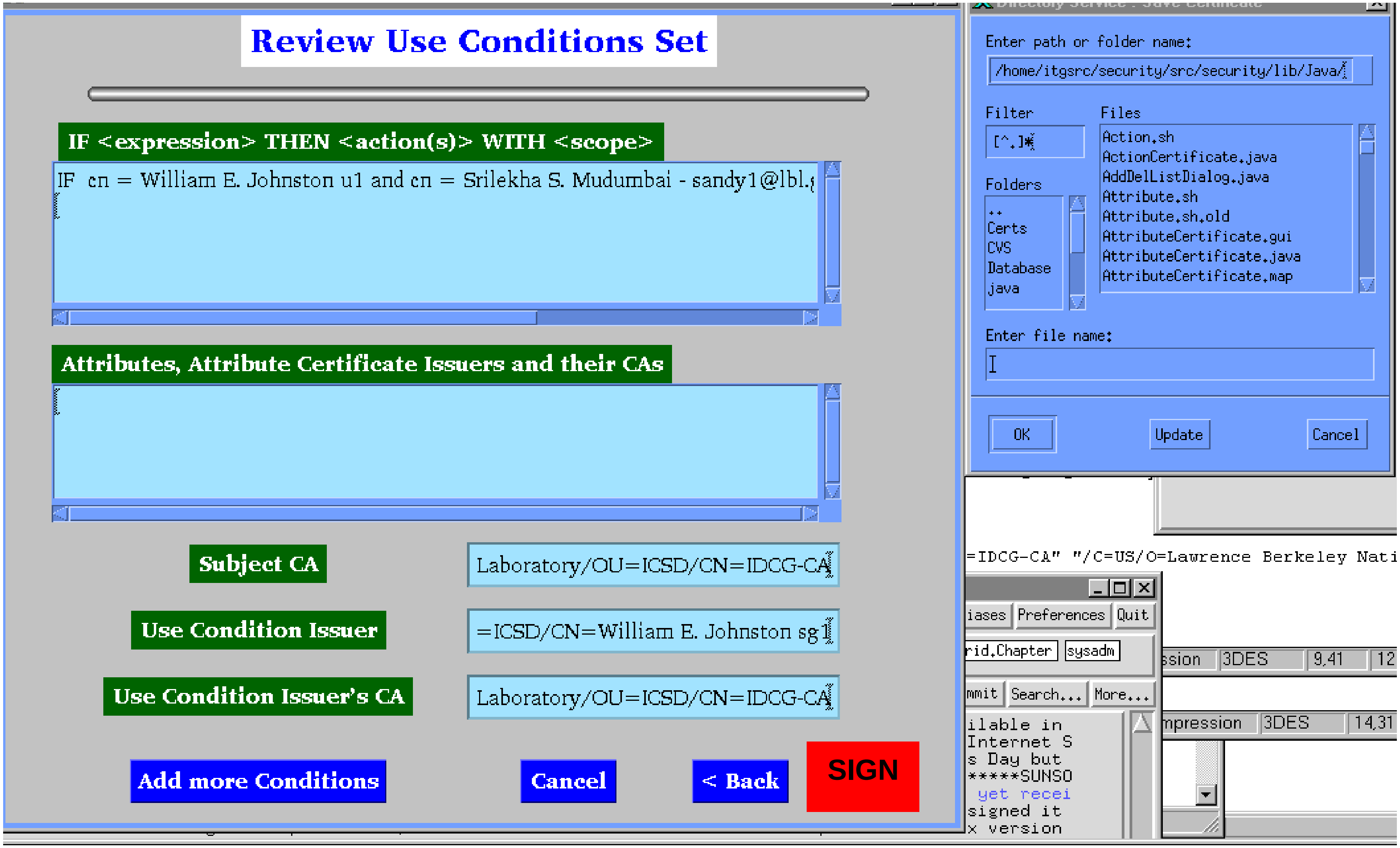
Scope of the Use Condition

Set scope of your use condition

The scope of the use condition may be applicable to only its level and/or its sub levels

- **For resources with a hierarchical policy model, the scope of the use-condition certificate must be specified.**

Certificate Infrastructure



Review Use Conditions Set

IF <expression> THEN <action(s)> WITH <scope>

IF cn = William E. Johnston u1 and cn = Srilekha S. Mudumbai - sandy1@lbl.g

Attributes, Attribute Certificate Issuers and their CAs

Subject CA: Laboratory/OU=ICSD/CN=IDCG-CA

Use Condition Issuer: =ICSD/CN=William E. Johnston sg1

Use Condition Issuer's CA: Laboratory/OU=ICSD/CN=IDCG-CA

Directory Service : Save Certificate

Enter path or folder name: /home/itgsrc/security/src/security/lib/Java/

Filter: [^.]*

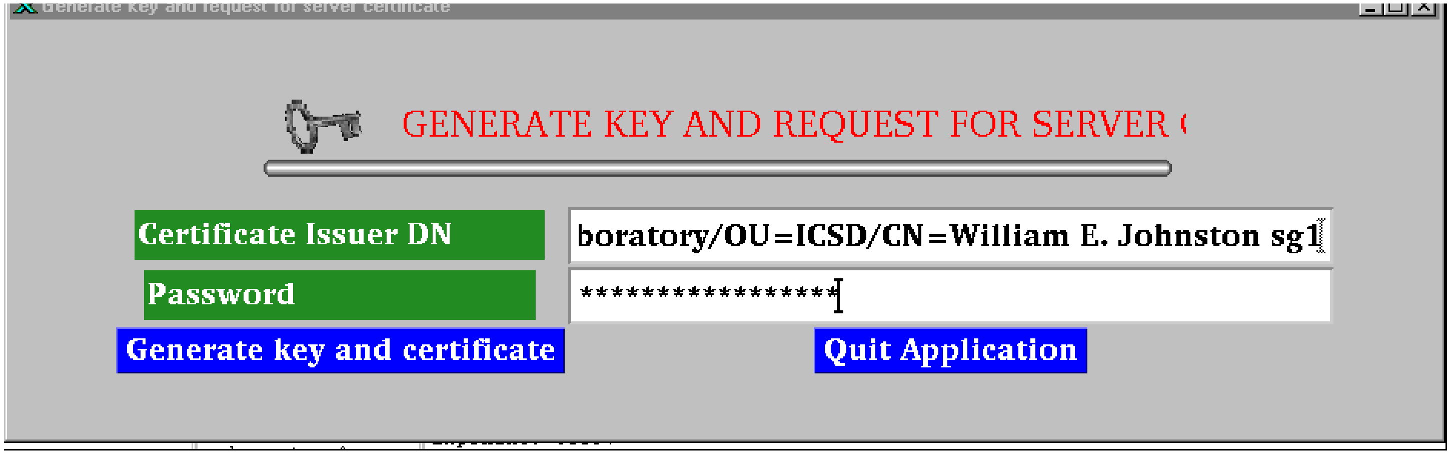
Folders:
..
Certs
CVS
Database
java

Files:
Action.sh
ActionCertificate.java
AddDelListDialog.java
Attribute.sh
Attribute.sh.old
AttributeCertificate.gui
AttributeCertificate.java
AttributeCertificate.map

Enter file name:

```
=IDCG-CA" "/C=US/O=Lawrence Berkeley Nati
ilable in
Internet S
s Day but
*****SUNSO
 yet recei
signed it
x version
```

Certificate Infrastructure

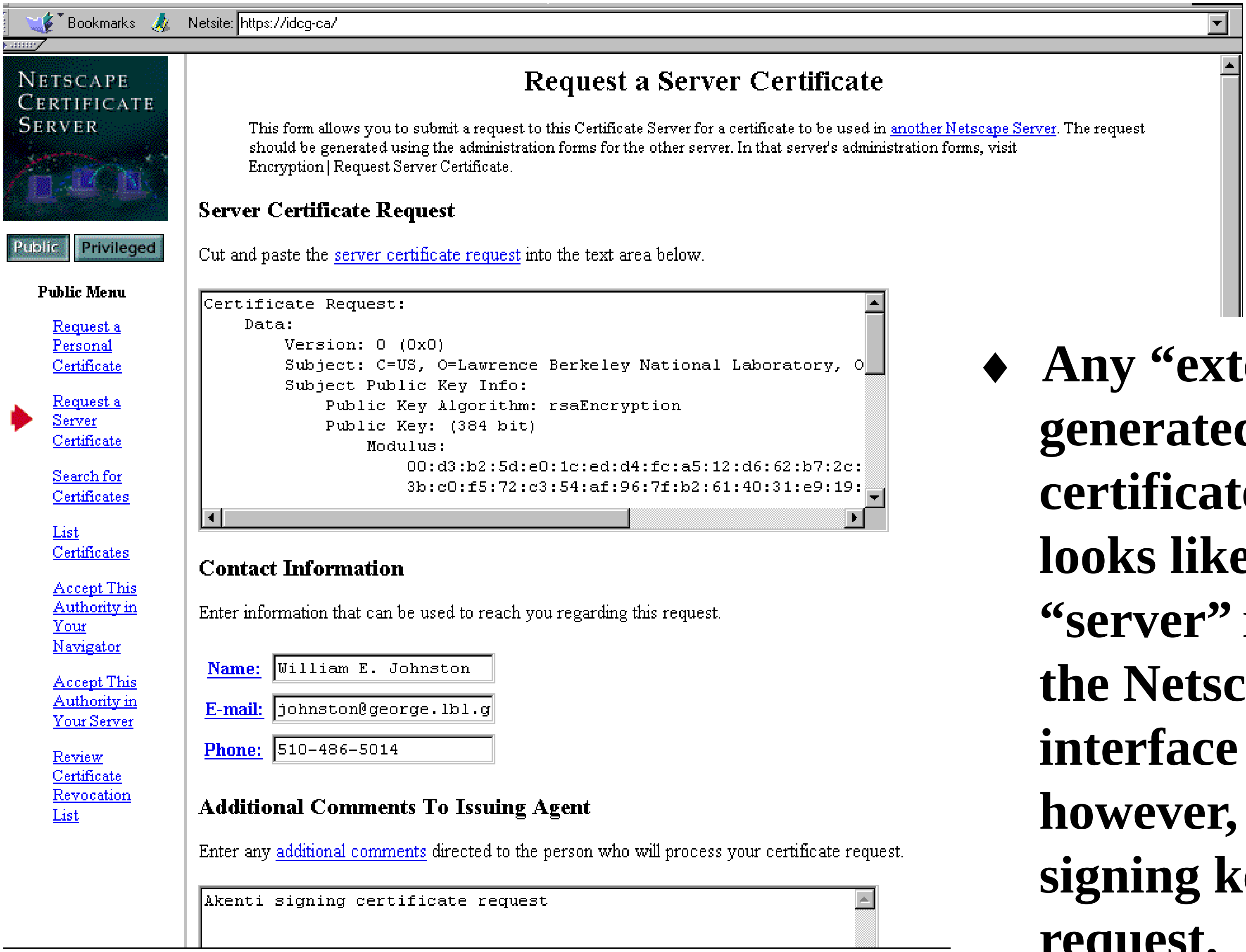

Generate key and request for server certificate
GENERATE KEY AND REQUEST FOR SERVER (
Generate key and certificate
Quit Application

Certificate Issuer DN: boratory/OU=ICSD/CN=William E. Johnston sg1

Password: *****************

- Signing key and certificate requests are generated by a program run in the issuer’s local environment
- The encrypted private key and the certificate request are kept in ~issuer/.Akenti
- Once the certificate for the signing identity is issued, the “identity” is portable - like Netscape v.4 private keys, it may be moved from system to system.

Certificate Infrastructure


Bookmarks
Netsite: https://idcg-ca/
NETSCAPE CERTIFICATE SERVER
Public
Privileged
Public Menu
Request a Personal Certificate
Request a Server Certificate
Search for Certificates
List Certificates
Accept This Authority in Your Navigator
Accept This Authority in Your Server
Review Certificate Revocation List

Request a Server Certificate

This form allows you to submit a request to this Certificate Server for a certificate to be used in another Netscape Server. The request should be generated using the administration forms for the other server. In that server's administration forms, visit Encryption | Request Server Certificate.

Server Certificate Request

Cut and paste the server certificate request into the text area below.

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=US, O=Lawrence Berkeley National Laboratory, O
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            Public Key: (384 bit)
                Modulus:
                    00:d3:b2:5d:e0:1c:ed:d4:fc:a5:12:d6:62:b7:2c:
                    3b:c0:f5:72:c3:54:af:96:7f:b2:61:40:31:e9:19:
```

Contact Information

Enter information that can be used to reach you regarding this request.

Name:	William E. Johnston
E-mail:	johnston@george.lbl.g
Phone:	510-486-5014

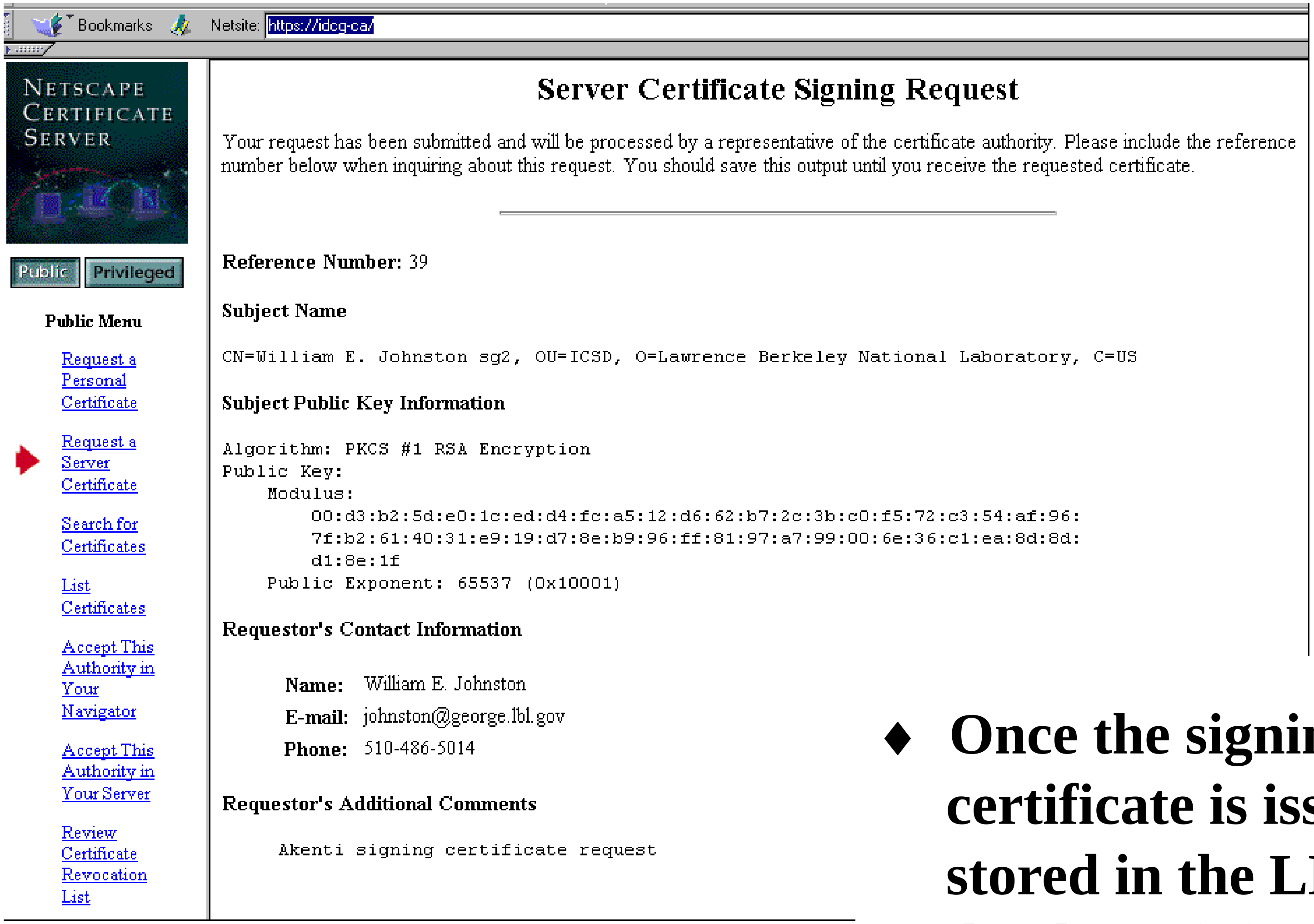
Additional Comments To Issuing Agent

Enter any additional comments directed to the person who will process your certificate request.

```
Akenti signing certificate request
```

- Any “externally” generated certificate request looks like a “server” request to the Netscape CA interface - this, however, is a signing key request.

Certificate Infrastructure


Bookmarks
Netsite: https://idcg-ca/
NETSCAPE CERTIFICATE SERVER
Public
Privileged
Public Menu
Request a Personal Certificate
Request a Server Certificate
Search for Certificates
List Certificates
Accept This Authority in Your Navigator
Accept This Authority in Your Server
Review Certificate Revocation List

Server Certificate Signing Request

Your request has been submitted and will be processed by a representative of the certificate authority. Please include the reference number below when inquiring about this request. You should save this output until you receive the requested certificate.

Reference Number: 39

Subject Name

```
CN=William E. Johnston sg2, OU=ICSD, O=Lawrence Berkeley National Laboratory, C=US
```

Subject Public Key Information

```
Algorithm: PKCS #1 RSA Encryption
Public Key:
    Modulus:
        00:d3:b2:5d:e0:1c:ed:d4:fc:a5:12:d6:62:b7:2c:3b:c0:f5:72:c3:54:af:96:
        7f:b2:61:40:31:e9:19:d7:8e:b9:96:ff:81:97:a7:99:00:6e:36:c1:ea:8d:8d:
        d1:8e:1f
    Public Exponent: 65537 (0x10001)
```

Requestor's Contact Information

Name:	William E. Johnston
E-mail:	johnston@george.lbl.gov
Phone:	510-486-5014

Requestor's Additional Comments

```
Akenti signing certificate request
```

- ♦ Once the signing certificate is issued and stored in the LDAP database, it is available for validating use-condition certificates

CDS: A Simple Akenti Application

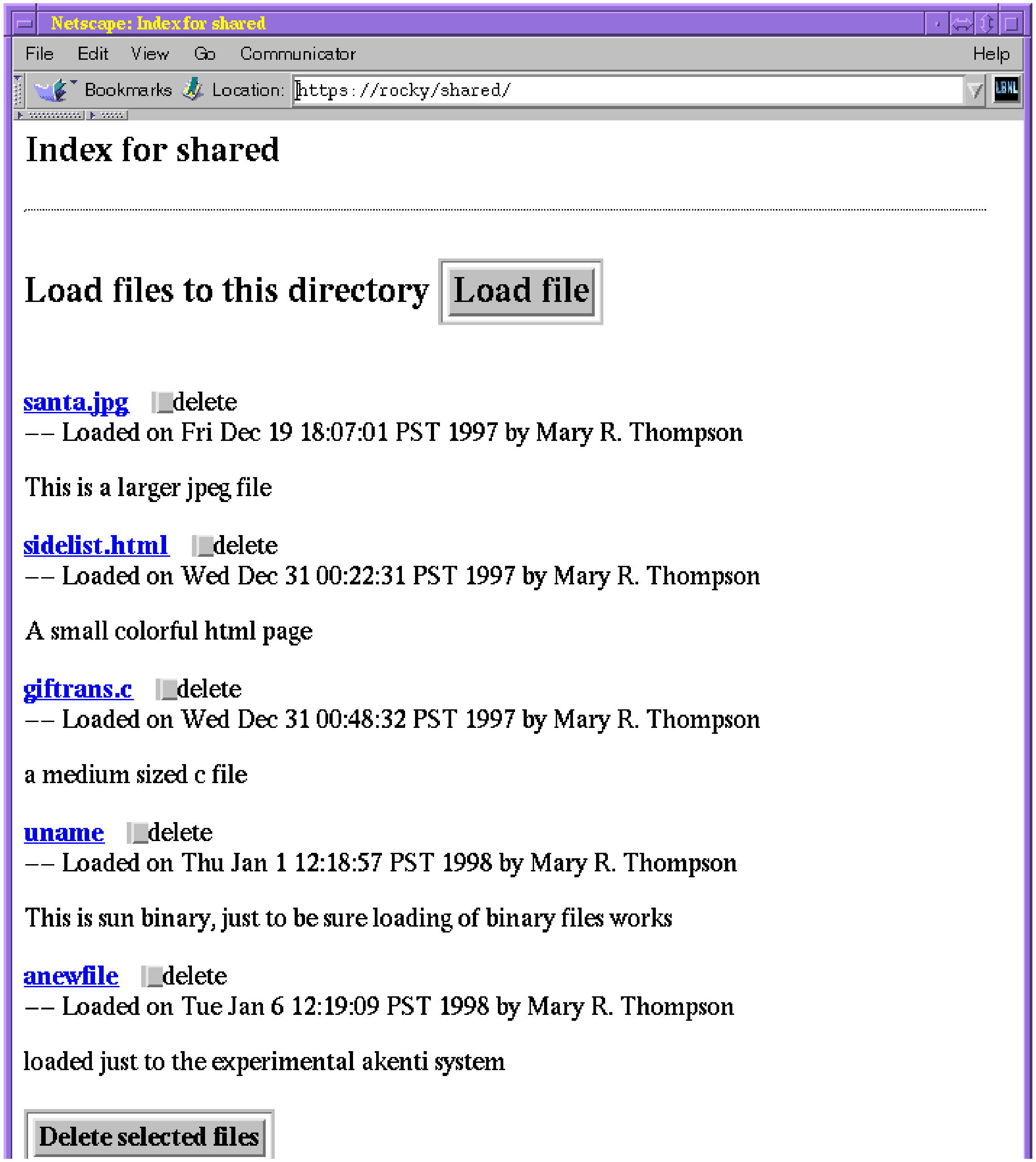
- **Access *Controlled Data Sharing***

CDS provides for uploading and downloading files to and from an area of a server that is access controlled by use-condition certificates.

The file may be described by a simple annotation.

The goal is a secure and easily used, group-oriented, data sharing facility.

Application



Index for shared

Load files to this directory

santa.jpg □ delete
–– Loaded on Fri Dec 19 18:07:01 PST 1997 by Mary R. Thompson

This is a larger jpeg file

sidelist.html □ delete
–– Loaded on Wed Dec 31 00:22:31 PST 1997 by Mary R. Thompson

A small colorful html page

giftrans.c □ delete
–– Loaded on Wed Dec 31 00:48:32 PST 1997 by Mary R. Thompson

a medium sized c file

uname □ delete
–– Loaded on Thu Jan 1 12:18:57 PST 1998 by Mary R. Thompson

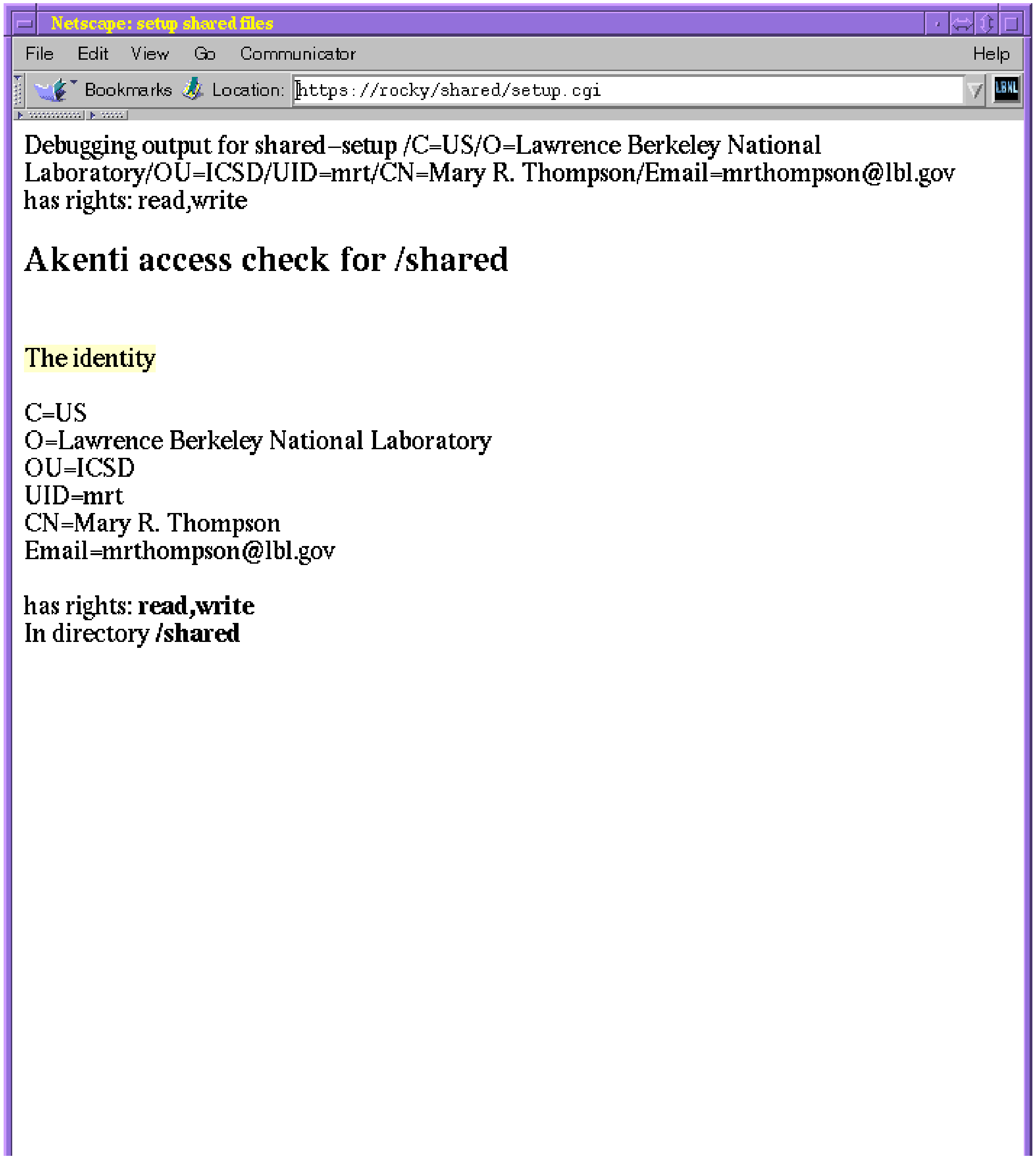
This is sun binary, just to be sure loading of binary files works

anewfile □ delete
–– Loaded on Tue Jan 6 12:19:09 PST 1998 by Mary R. Thompson

loaded just to the experimental akenti system

User view of CDS annotated file directory.

Application



Debugging output for shared–setup /C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/UID=mrt/CN=Mary R. Thompson/Email=mrthompson@lbl.gov has rights: read,write

Akenti access check for /shared

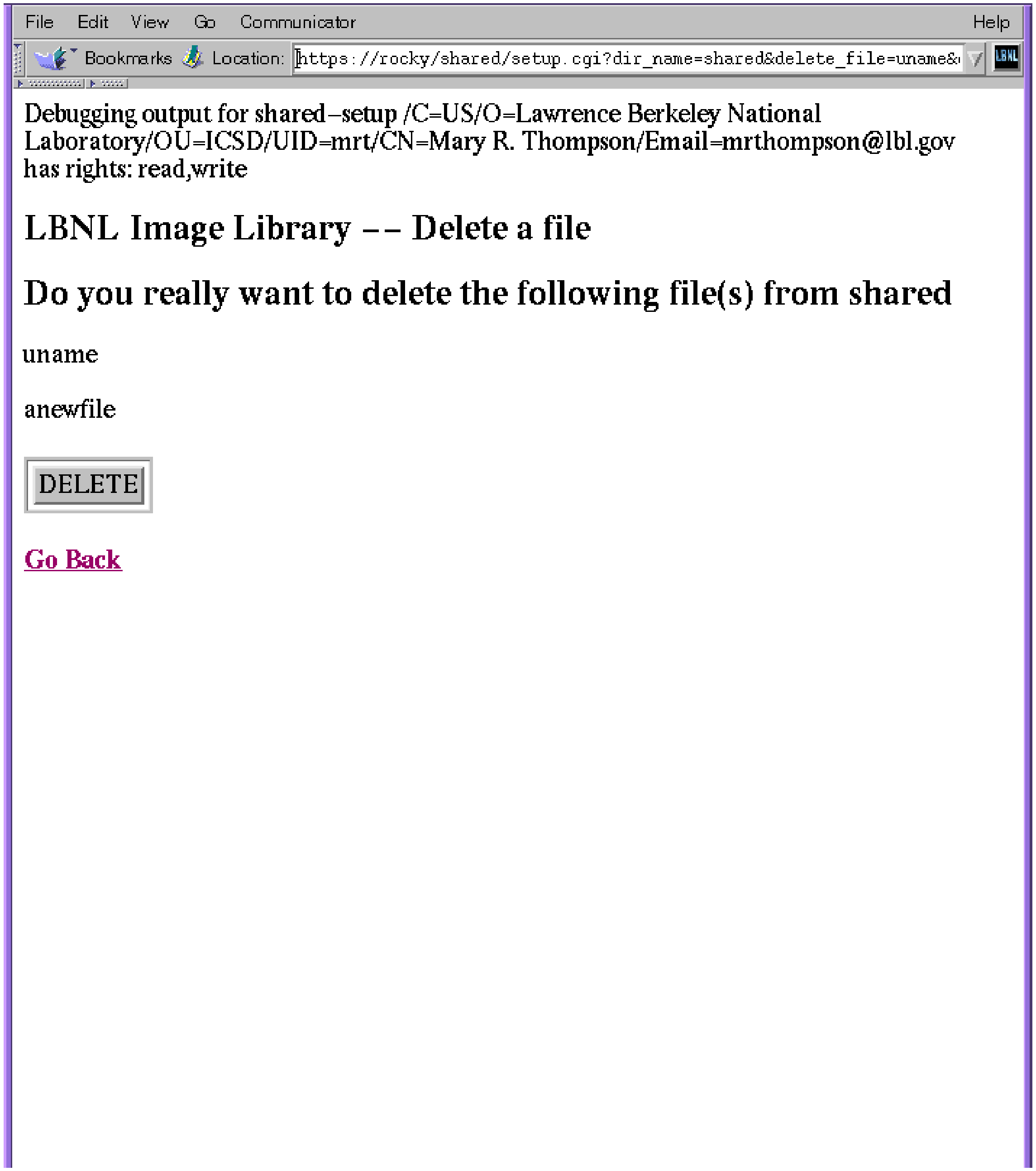
The identity

C=US
O=Lawrence Berkeley National Laboratory
OU=ICSD
UID=mrt
CN=Mary R. Thompson
Email=mrthompson@lbl.gov

has rights: **read,write**
In directory **/shared**

The user can query the current access rights.

Application


File
Edit
View
Go
Communicator
Help
Bookmarks
Location:
https://rocky/shared/setup.cgi?dir_name=shared&delete_file=uname&

Debugging output for shared–setup /C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/UID=mrt/CN=Mary R. Thompson/Email=mrthompson@lbl.gov has rights: read,write

LBNL Image Library –– Delete a file

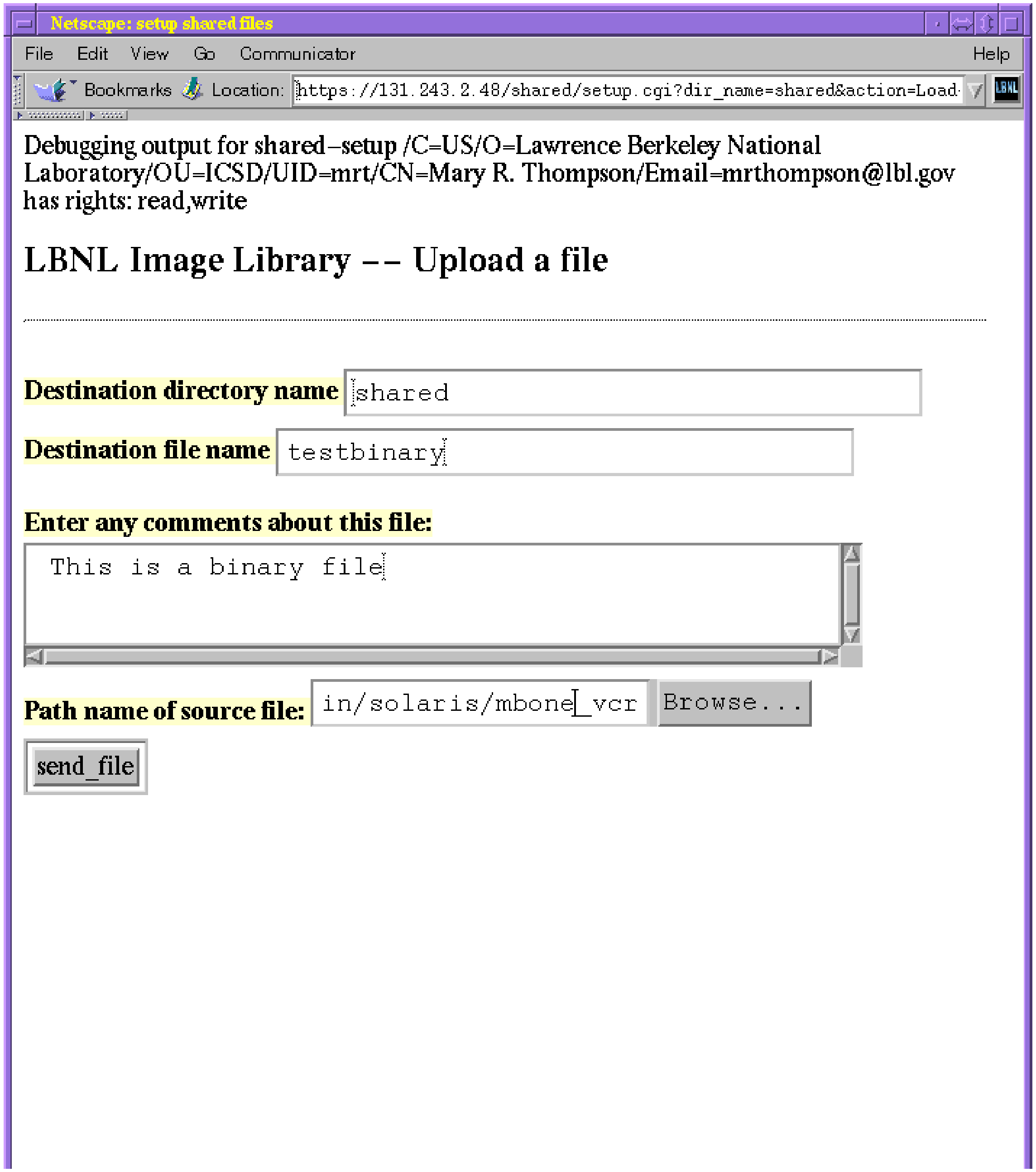
Do you really want to delete the following file(s) from shared

uname

anewfile

Delete capability is granted separately from access.

Application



Netscape: setup shared files
File Edit View Go Communicator Help
Bookmarks Location:

https://131.243.2.48/shared/setup.cgi?dir_name=shared&action=Load·

Debugging output for shared–setup /C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/UID=mrt/CN=Mary R. Thompson/Email=mrthompson@lbl.gov has rights: read,write

LBNL Image Library –– Upload a file

Destination directory name: shared

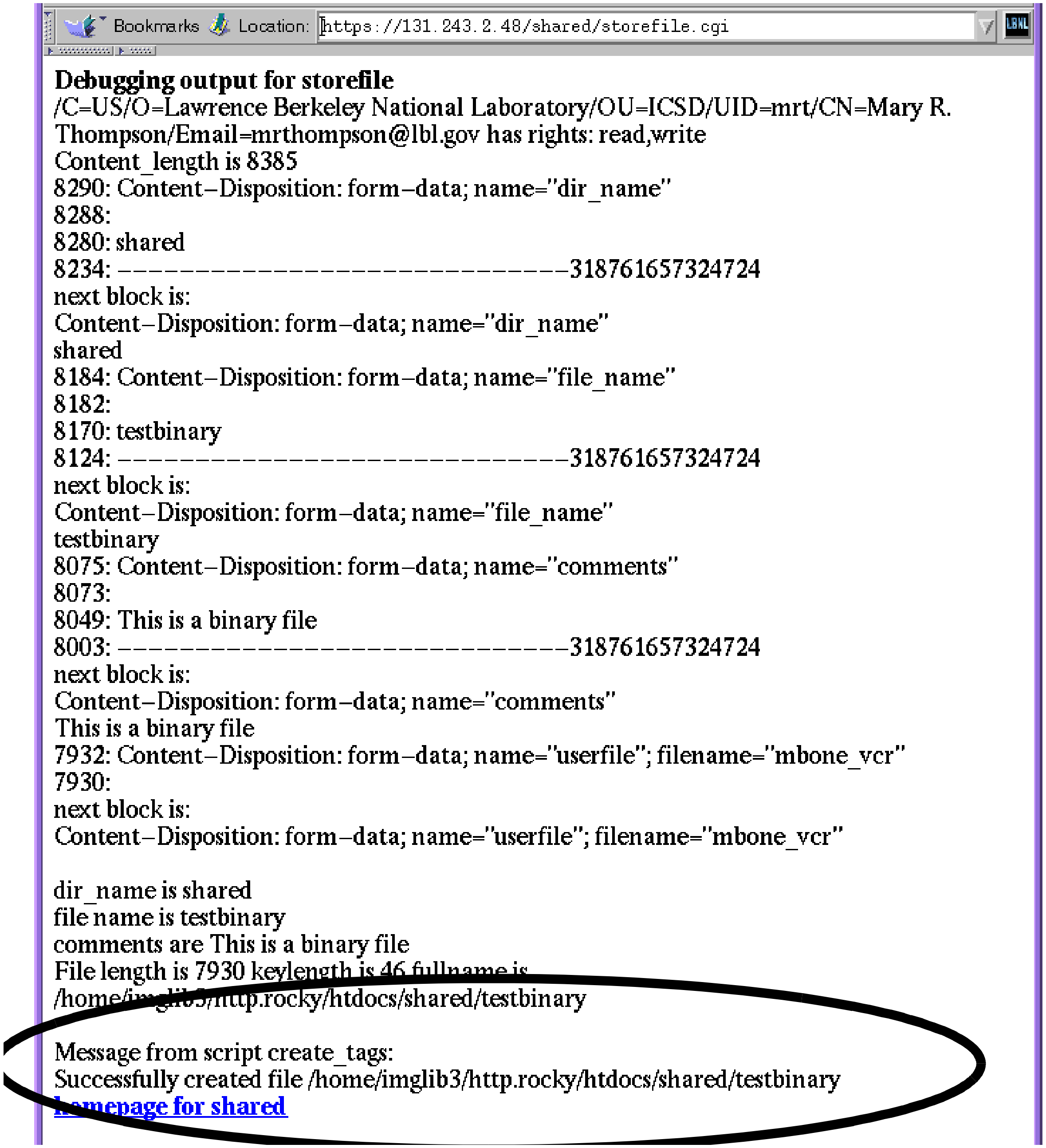
Destination file name: testbinary

Enter any comments about this file: This is a binary file

Path name of source file: in/solaris/mbone_vcr

Upload is intended to be simple, and provides for free-form user description of the file.

Application



https://131.243.2.48/shared/storefile.cgi

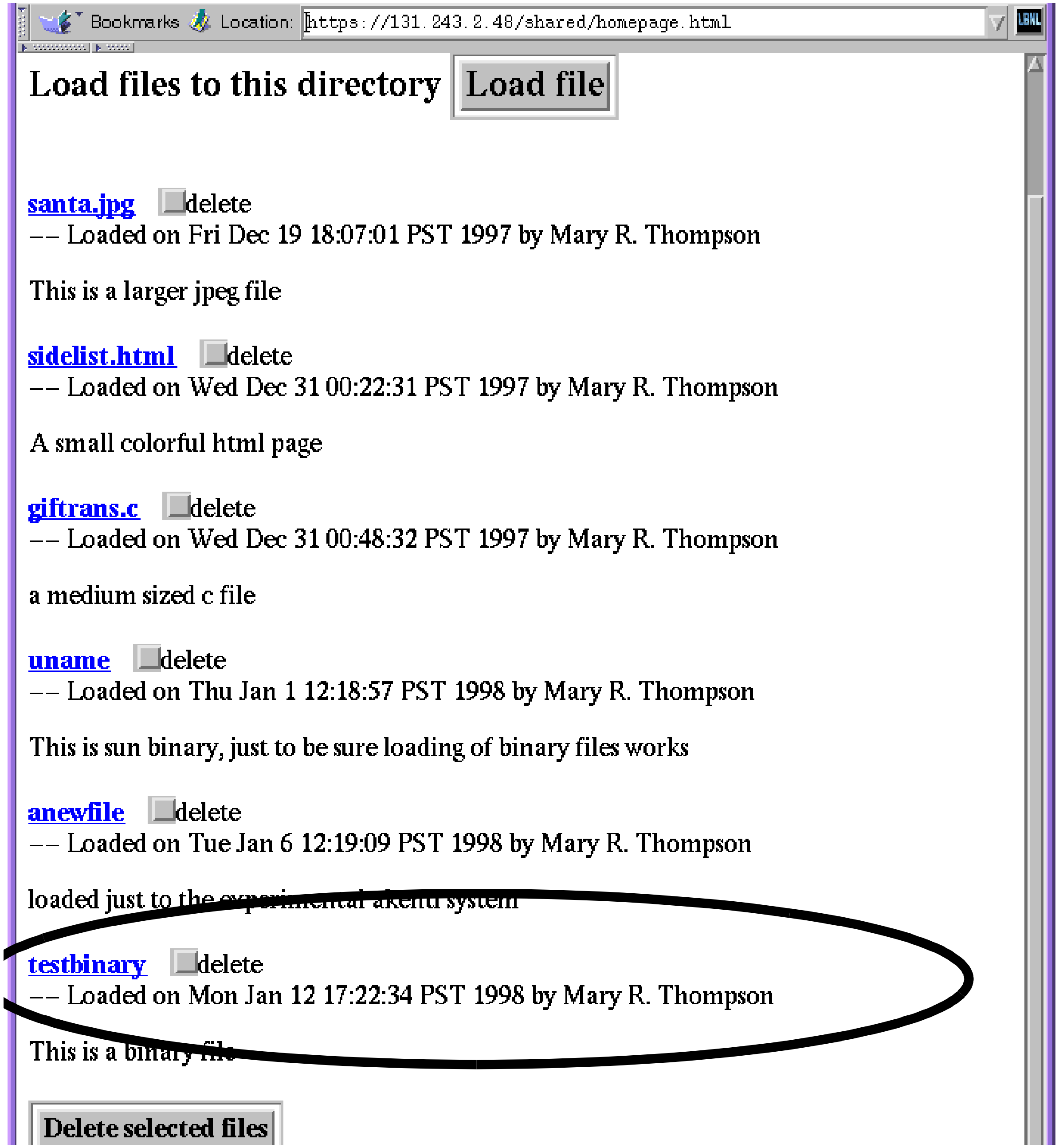
Debugging output for storefile

```
/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/UID=mrt/CN=Mary R.
Thompson/Email=mrthompson@lbl.gov has rights: read,write
Content_length is 8385
8290: Content-Disposition: form-data; name="dir_name"
8288:
8280: shared
8234: -----------------------------318761657324724
next block is:
Content-Disposition: form-data; name="dir_name"
shared
8184: Content-Disposition: form-data; name="file_name"
8182:
8170: testbinary
8124: -----------------------------318761657324724
next block is:
Content-Disposition: form-data; name="file_name"
testbinary
8075: Content-Disposition: form-data; name="comments"
8073:
8049: This is a binary file
8003: -----------------------------318761657324724
next block is:
Content-Disposition: form-data; name="comments"
This is a binary file
7932: Content-Disposition: form-data; name="userfile"; filename="mbone_vcr"
7930:
next block is:
Content-Disposition: form-data; name="userfile"; filename="mbone_vcr"

dir_name is shared
file name is testbinary
comments are This is a binary file
File length is 7930 keylength is 46 fullname is
/home/imglib3/http.rocky/htdocs/shared/testbinary

Message from script create_tags:
Successfully created file /home/imglib3/http.rocky/htdocs/shared/testbinary
```

homepage for shared

Filtering the audit log will provide user feedback.

Application



Location: https://131.243.2.48/shared/homepage.html

Load files to this directory

santa.jpg □delete
–– Loaded on Fri Dec 19 18:07:01 PST 1997 by Mary R. Thompson

This is a larger jpeg file

sidelist.html □delete
–– Loaded on Wed Dec 31 00:22:31 PST 1997 by Mary R. Thompson

A small colorful html page

giftrans.c □delete
–– Loaded on Wed Dec 31 00:48:32 PST 1997 by Mary R. Thompson

a medium sized c file

uname □delete
–– Loaded on Thu Jan 1 12:18:57 PST 1998 by Mary R. Thompson

This is sun binary, just to be sure loading of binary files works

anewfile □delete
–– Loaded on Tue Jan 6 12:19:09 PST 1998 by Mary R. Thompson

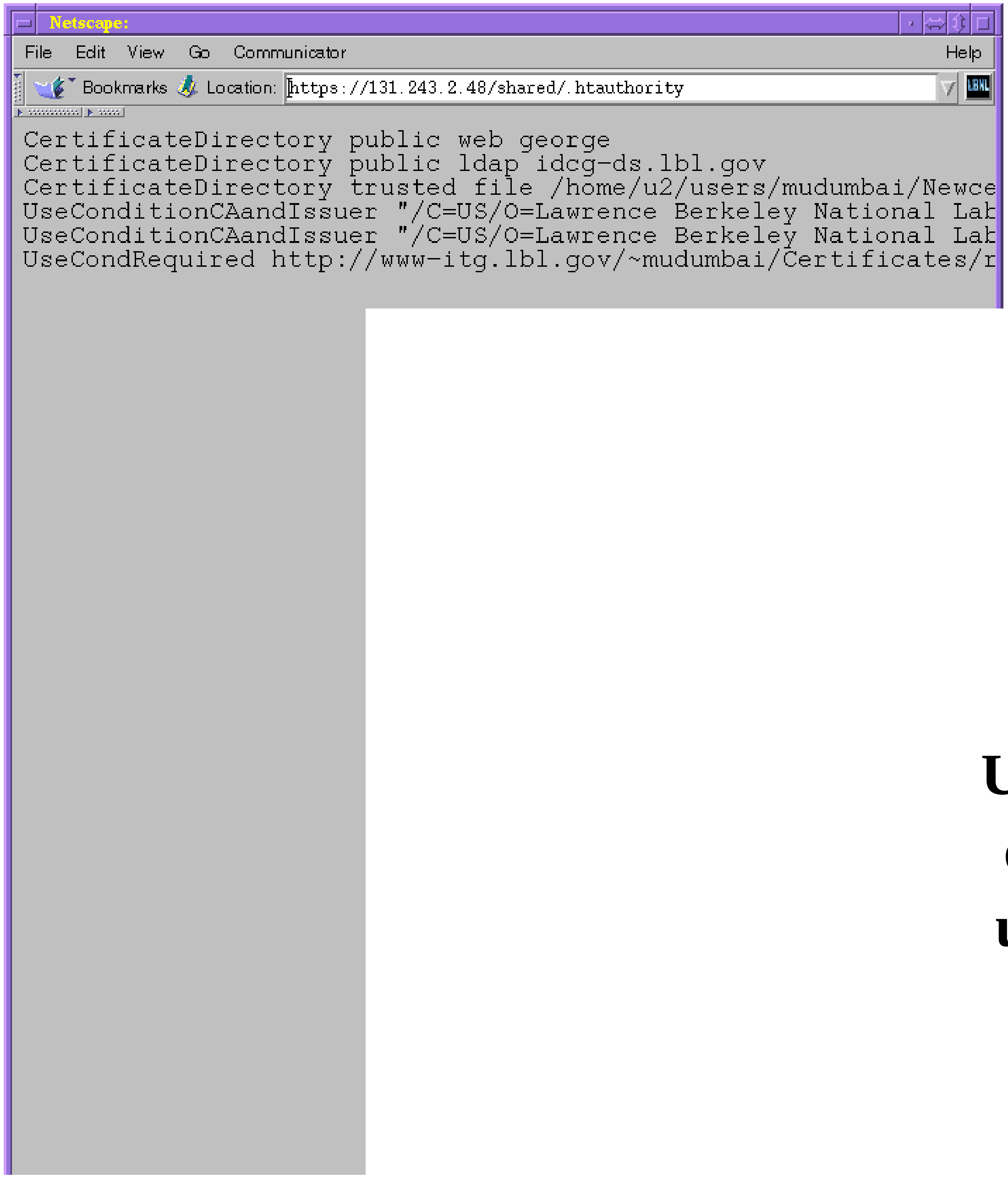
loaded just to the experimental akenti system

testbinary □delete
–– Loaded on Mon Jan 12 17:22:34 PST 1998 by Mary R. Thompson

This is a binary file

A new shared file has been created.

Application



https://131.243.2.48/shared/.htauthority

```
CertificateDirectory public web george
CertificateDirectory public ldap idcg-ds.lbl.gov
CertificateDirectory trusted file /home/u2/users/mudumbai/Newce
UseConditionCAandIssuer "/C=US/O=Lawrence Berkeley National Lab
UseConditionCAandIssuer "/C=US/O=Lawrence Berkeley National Lab
UseCondRequired http://www-itg.lbl.gov/~mudumbai/Certificates/r
```

Users will be able to query who defines use-conditions, but not the specific use-condition.